21世纪高等学校网络空间安全专业规划教材



云南省普通高等学校“十二五”规划教材

信息安全工程

◎ 林英 康雁 张一凡 朱艳萍 张雁 编著

清華大学出版社

21 世纪高等学校网络空间安全专业规划教材

信息安全工程

林　英　康　雁　张一凡　朱艳萍　张　雁　编著

清华大学出版社

北　京

内 容 简 介

本书以信息安全工程理论为基础，以实际工程应用为目标，对信息安全从规划与控制、需求与分析、实施与评估等工程过程进行描述，并结合具体信息安全工程案例的实现，介绍信息安全工程的内容。

本书首先介绍安全工程基础，涉及软件/系统工程基础、质量管理基础、能力成熟度模型基础以及项目管理基础等内容；其次介绍安全工程过程实践，涉及信息系统安全工程（ISSE）、系统安全工程能力成熟度模型（SSE-CMM）、信息安全工程实施、信息安全风险评估等内容；最后介绍项目管理过程和实践，涉及数据备份与灾难恢复、生命周期安全支持以及信息安全工程管理等内容。

本书概念清晰，层次分明，内容涉及的范围比较广，不仅适合作为信息安全专业及相关专业的教学用书，还适合对安全工程技术感兴趣的人员阅读。

图书在版编目（CIP）数据

信息安全工程/林英等编著.—北京：清华大学出版社，2019
（21世纪高等学校网络空间安全专业规划教材）
ISBN 978-7-302-52505-9

Ⅰ.①信…　Ⅱ.①林…　Ⅲ.①信息安全—安全工程—高等学校—教材　Ⅳ.①TP309

中国版本图书馆CIP数据核字(2019)第109729号

责任编辑：黄　芝　张爱华
封面设计：刘　键
责任校对：李建庄
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**15　　**字　　数：**364千字
版　　次：2019年9月第1版　　**印　　次：**2019年9月第1次印刷
印　　数：1～1500
定　　价：39.90元

产品编号：078251-01

前　　言

随着经济和信息化的发展，信息资源已成为社会发展的重要战略资源，信息技术和信息产业正在改变传统的生产和生活方式，逐步成为国家经济增长的主要推动力之一。信息化、网络化的发展已成为不可阻挡、不可回避、不可逆转的历史潮流，信息技术和信息的开发应用已渗透到国家政治、经济、军事和社会生活的各个方面，成为生产力的重要因素。

信息时代人们在享受其所带来的种种物质和文化享受的同时，也受到日益严重的来自网络的安全威胁，如数据窃取、黑客入侵、病毒发布。尽管人们正在广泛地使用各种复杂的软件技术，如防火墙、入侵检测、访问控制，但黑客活动越来越猖狂，无孔不入，对社会造成了严重的危害。可以说，信息化发展程度越高，面临的信息安全风险就越大。信息安全的建设实际上是一个复杂的系统工程。它要综合利用数学、物理、通信和计算机等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，加强顶层设计，提出系统的、完整的、协同的解决方案。安全问题的解决，不能只依靠纯粹的技术和简单的安全产品的堆砌，也不能仅靠安全管理体系建设。安全问题的解决也是一个复杂的系统工程，需要采用工程的概念、原理、技术和方法来研究、开发、实施与维护信息系统安全。因此，把信息安全作为一个整体的工程进行研究，具有重要的现实意义。

本书共分10章。第1章绪论，阐述信息安全基本属性及信息安全工程的发展由来；第2章信息安全工程基础，介绍信息安全工程相关的一些理论基础，如系统工程思想、项目管理方法及质量管理体系；第3章信息系统安全工程，详细介绍信息系统安全工程(ISSE)方法论；第4章SSE-CMM，详细介绍系统安全工程-能力成熟度模型(SSE-CMM)；第5章信息安全风险管理与风险评估，介绍风险管理与风险评估的相关概念及实施流程和方法；第6章信息安全管理，介绍信息安全管理的相关概念及常用的一些信息安全管理模型；第7章安全层次划分，主要介绍如何从安全的密码算法、安全协议、网络安全、系统安全及应用安全等方面来探讨安全解决方案；第8章信息安全事件应急处理与灾难恢复，介绍信息安全事件应急处理与灾难恢复过程；第9章信息安全标准与法律法规，介绍信息安全相关标准与信息安全相关法律法规；第10章信息安全工程案例，以信息安全工程理论为基础，结合一个具体的信息安全工程案例的实现，以实际工程应用为目标，对信息安全从规划与控制、需求与分析、实施与评估等工程过程进行描述。

本书主要总结了多年信息安全工程本科教学的内容，同时还参考了近年来的文献资料。

在写作中，力求做到层次清楚，语言简洁流畅，内容丰富，既便于读者循序渐进地系统学习，又能使读者了解信息安全工程理论的新发展。希望本书对读者了解信息安全工程有一定帮助。

本书的第1、3、5、10章由林英执笔完成，第2、4章由康雁执笔完成，第6、7章由张一凡执笔完成，第8、9章由朱艳萍执笔完成，全书由林英、张雁统稿。

本书的完成，得到了云南省“十二五质量工程”项目的资助，在此谨表衷心的感谢。

限于学术水平，书中不妥之处在所难免，敬请读者批评指正，作者将不胜感激。

作　者

2019年6月

目　　录

第1章　绪　　论

本章学习目标：

- 了解信息安全的基本概念。
- 了解信息安全工程的基本概念。
- 掌握信息安全体系模型。

1.1　信息安全基础

1.1.1　信息安全的基本概念

随着经济和信息化的发展，信息资源已成为社会发展的重要战略资源，信息技术和信息产业正在改变传统的生产和生活方式，逐步成为国家经济增长的主要推动力之一。

信息时代在给人们带来种种物质和文化享受的同时，人们也受到日益严重的来自网络的安全威胁，如数据窃取、黑客入侵、病毒发布。尽管人们正在广泛地使用各种复杂的软件技术，如防火墙、入侵检测、访问控制，但黑客活动越来越猖狂，无孔不入，对社会造成了严重的危害。

可以说，信息化发展程度越高，面临的信息安全风险就越大。信息安全的建设实际上是一个复杂的系统工程。它需要综合利用数学、物理、通信和计算机等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，加强顶层设计，提出系统的、完整的、协同的解决方案。

1. 信息安全的定义

首先来看信息的定义，关于信息，目前理论界中尚无定论。控制论的创始人维纳(Norbert Wiener)认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”。信息论的奠基人香农认为“信息是用来消除随机不确定性的东西”。我国信息论专家钟义信教授把信息定义为事物运动的状态与方式。在ISO/IEC TR 13335，即《IT安全管理指南》中，信息是指通过在数据上施加某些约定而赋予这些数据的特殊含义。对现代企业来说，信息是一种资产，既包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章、关键人员等。

什么是安全？安全同样没有一个统一的定义。人们对安全所下的各种定义如下。

(1) 安全是指客观事物的危险程度能够为人们普通接受的状态。

(2) 安全是指没有引起死亡、伤害、职业病或财产、设备的损坏又或环境危害的条件。

(3) 安全是指不因人、机、媒介的相互作用而导致系统损失、人员伤害、任务受影响或造成的损失。

古人云：“无危则安，无损则全”就是说生产过程中没有危险，没有发生伤害或损坏的事

件，就叫作安全。

可以说，安全是生产过程中人、机、环境、物料等和谐运作的一种状态。安全是相对的，因为从科学角度讲，绝对安全的状态在客观上是不存在的，任何事物都包含有不安全的因素，具有一定的危险性。安全是信息的度量，因为安全不再单纯以功能或机制的强度作为评判指标，而是结合了应用环境和应用需求，使信息系统的使用者确信其预期的安全目标已获满足。

信息安全同样也没有公认和统一的定义。在美国《联邦信息安全管理法》中，信息安全指保护信息和信息系统，防止未经授权的访问、使用、泄露、中断、修改或破坏，以提供完整性、保密性及可用性。ISO 17799 从四个方面定义信息安全：保护信息免受各方威胁；确保组织业务连续性；将信息不安全带来的损失降低到最小；获得最大的投资回报和商业机会。

总之，信息安全的概念是随着信息技术的发展而不断拓展、不断深化的。信息安全概念的外延在不断扩大，内涵在不断丰富，在历史发展各个阶段所强调的重点不同，经历了不同的发展演变过程。

2. 信息安全基本属性

信息安全的三个重要的基本属性被称为信息安全金三角，即所谓的 CIA（Confidentiality-Integrity-Availability）金三角。CIA 模型如图 1-1 所示。

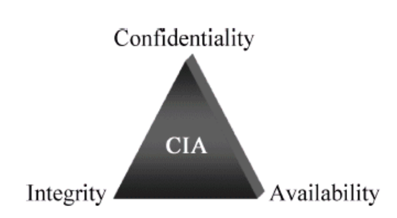


图 1-1 CIA 模型

（1）Confidentiality 即机密性。机密性也被称为保密性，是指信息不被泄露给非授权的用户、实体、进程，或被其利用的特性。机密性确保只有那些被授予特定权限的人才能够访问到信息。机密性包括信息内容的保密及信息状态的保密。常用的技术手段有防侦收、防辐射、信息加密、物理保密、信息隐藏等。

（2）Integrity 即完整性。完整性是指信息未经授权不能进行更改的特性，也就是信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。设备故障、误码、人为攻击、计算机病毒等是破坏完整性的主要因素。协议、纠错编码方法、密码校验和方法、数字签名、公证等是保证完整性的主要机制。

（3）Availability 即可用性。可用性是指信息可被授权实体访问并按需求使用的特性，即用户在需要时就可以使用所需的信息。信息的可用性涉及面较广，涉及硬件可用性、软件可用性、人员可用性及环境可用性等。可用性目前没有理论模型，是一种综合性的度量。对可用性的攻击就是阻断信息的可用，例如 DDoS 攻击的目的就是破坏目标系统的可用性。

机密性、完整性、可用性这三大基本属性也是信息安全的基本目标，然而，这三大目标之间又相互矛盾：机密性要求数据访问者少；完整性要求数据的同步、变化的共知；可用性要求读取数据方便，没有频繁的验证。因此，“安全”与“方便”常常是有矛盾的。为了取得这三大基本属性的安全，需要进行一些平衡和考虑。

除了上面介绍的三个基本属性之外，还有其他一些属性也用于描述信息安全的不同特性，如真实性、可控性、合法性、实用性、占有性、唯一性、不可否认性、可追溯性、生存性、稳定性、可靠性、特殊性等。其中，真实性反映的是主体身份、行为及相关信息的真实有效；可控性反映的是信息系统不会被非授权使用，信息的流动可以被选择性阻断；合法性反映的是

信息或信息系统的行为获得了授权;实用性反映的是信息加密密钥与信息的强关联性及密钥不可丢失的特性;占有性反映的是信息载体不可被盗用,确保由合法信息所占有;唯一性反映的是各信息以及信息系统行为主体之间不会出现混淆;不可否认性反映的是所生成的信息或信息系统的合法行为不会被抵赖;可追溯性反映的是信息系统的行为具有被审计的能力;生存性反映的是信息系统在受到攻击时可以通过采取降级等措施以保持最低限度的核心服务能力;稳定性反映的是信息系统不会出现异常情况;可靠性反映的是信息系统能够保持正常运行而不受外界影响的能力;特殊性反映的是信息所需要表现的特定内涵。

在诸多信息安全的属性中,机密性、真实性、可控性、可用性属于基本属性,相互不能蕴含。而其他属性,包括实用性、完整性、合法性、唯一性、不可否认性、特殊性、占有性、可追溯性、生存性、稳定性、可靠性等,则属于上述四个基本属性的某个侧面的突出反映,因此可以归结为这四个基本属性之中。其中实用性反映的是机密性在密钥依赖方面的机密属性;完整性、合法性、唯一性、不可否认性、特殊性分别反映的是真实性在信息内容本身、信息来源、信息系统行为主体、信息的发布行为、信息熵方面的真实属性;占有性、可追溯性分别反映的是可控性对信息资源的保护、对信息及信息系统行为的审计能力;生存性、稳定性、可靠性分别反映的是可用性在信息系统的容灾能力、信息系统的健壮能力、信息系统的可靠能力方面的可用属性。因此,机密性、真实性、可控性、可用性这四个基本属性实际上就是信息安全的四个核心属性,可以反映出信息安全的基本概貌。相对信息安全金三角而言,业界著名的信息安全专家方滨兴院士在深入分析和继承了传统信息安全定义的前提下,根据当前国际信息安全的发展现状,给出了信息安全四要素,并重新概括和界定了信息安全的内涵和外延。信息安全四要素简称CACA,即机密性(Confidentiality)、真实性(Authenticity)、可控性(Controllability)和可用性(Availability)。

3. 信息安全基本属性与信息安全层次模型的关系

了解了信息安全的一些基本属性后,人们可以认识信息安全的这些基本属性与人们平时所关注的每个层次的安全有什么样的对应以及一些相应的处理办法。

(1) 物理安全。物理安全是指对网络与信息系统的物理装备的保护,主要涉及网络与信息系统的机密性、可用性、完整性、生存性、稳定性、可靠性等基本属性。所面对的威胁主要包括电磁泄漏、通信干扰、信号注入、人为破坏、自然灾害、设备故障等。主要的保护方式有加扰处理、电磁屏蔽、数据校验、容错、冗余、系统备份等。

(2) 运行安全。运行安全是指对网络与信息系统的运行过程和运行状态的保护,主要涉及网络与信息系统的真实性、可控性、可用性、合法性、唯一性、可追溯性、占有性、生存性、稳定性、可靠性等。所面对的威胁包括非法使用资源、系统安全漏洞利用、网络阻塞、网络病毒、越权访问、非法控制系统、黑客攻击、拒绝服务攻击、软件质量差、系统崩溃等。主要的保护方式有防火墙与物理隔离、风险分析与漏洞扫描、应急响应、病毒防治、访问控制、安全审计、入侵检测、源路由过滤、降级使用、数据备份等。

(3) 数据安全。数据安全是指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护,使得在数据处理层面保障信息依据授权使用,不被非法冒充、窃取、篡改、抵赖,主要涉及信息的机密性、真实性、实用性、完整性、唯一性、不可否认性、生存性等;所面对的威胁包括窃取、伪造、密钥截获、篡改、冒充、抵赖、攻击密钥等。主要的保护方式有加密、认证、非对称密钥、完整性验证、鉴别、数字签名、秘密共享等。

(4) 内容安全。内容安全是指对信息在网络内流动中的选择性阻断,以保证信息流动的可控能力。在此,被阻断的对象是通过内容可以判断出来的对系统造成威胁的脚本病毒、因无限制扩散而导致消耗用户资源的垃圾类邮件、导致社会不稳定的有害信息等。主要涉及信息的机密性、真实性、可控性、可用性、完整性、可靠性等。所面对的难题包括信息不可识别(因加密)、信息不可更改、信息不可阻断、信息不可替换、信息不可选择、系统不可控等。主要的处理办法是密文解析或形态解析、流动信息的裁剪、信息的阻断、信息的替换、信息的过滤、系统的控制等。

(5) 信息对抗。信息对抗是指在信息的利用过程中,对信息熵的真实性的隐藏与保护,或者攻击与分析。主要涉及信息熵的机密性、完整性、特殊性等。所面对的主要问题包括多角度综合分析、攻击或压制信息的传递,用无用信息来干扰信息熵的本质。主要的处理办法是消隐重要的局部信息,加大信息获取能力,消除信息的不确定性等。

1.1.2 信息安全发展过程

在 20 世纪四五十年代,人们认为信息安全就是通信安全,因为当时电报、电话、无线通信的大量应用,特别是二次大战的需求,必须考虑秘密消息在传输途中被除发信者和收信者以外的第三者截获的可能性,考虑即使截获者截获信息的载体,如文本、无线电波等,也无法得知其中的内容,这个时期,信息安全进入了通信保密 Communication Security 阶段。

在通信保密发展阶段,搭线窃听及密码学分析是主要的安全威胁,因此必须考虑如何保障信息的机密性,研究如何对信息进行编码后在通信信道上传输,防止攻击者通过窃听通信信道而获取信息。1949 年香农发表的《保密系统的信息理论》和 1977 年美国国家标准局公布的数据加密标准(Data Encryption Standard,DES)是信息安全这一发展阶段的时代标志,主要的防护措施是数据加密。

进入 20 世纪 70 年代,通信保密阶段转变到计算机安全(Computer Security)阶段,这一时期的标志是 1977 年美国国家标准局公布的《数据加密标准》(DES)和 1985 年美国国防部公布的《可信计算机系统评估准则》(TCSEC),这些标准的提出意味着解决信息系统保密性问题的研究和应用迈上了历史的新台阶。

进入 20 世纪 80 年代后,计算机的性能得到了成百上千倍的提高,应用的范围也在不断扩大,计算机已遍及世界各个角落,人们正努力利用通信网络把孤立的单机系统连接起来,相互通信和共享资源。但随之而来并日益严峻的问题是计算机中信息的安全问题。由于计算机中信息有共享和易于扩散等特性,它在处理、存储、传输和使用上有着严重的脆弱性,很容易被干扰、滥用、遗漏和丢失,甚至被泄露、窃取、篡改、伪造和破坏,因此人们开始关注计算机系统中的硬件、软件及在处理、存储、传输信息中的保密性。这个阶段主要的手段是通过访问控制,防止对计算机中信息的非授权访问,从而保护信息的保密性。但是,随着计算机病毒、计算机软件 Bug 等问题的不断显现,保密性已经不能满足人们对计算机安全的需求,完整性和可用性等新的计算机安全需求走上舞台。

进入 20 世纪 90 年代之后,信息系统安全(Information System Security)开始成为信息安全的核心内容。此时,通信和计算机技术已经相互依存,计算机网络发展成为全天候、通全球、个人化、智能化的信息高速公路,互联网成了寻常百姓可及的家用技术平台,安全的需求不断地向社会的各个领域扩展,人们的关注对象从计算机转向更具本质性的信息本身,继

而关注信息系统的安全。人们需要保护信息在存储、处理或传输过程中不被非法访问或更改,确保对合法用户的服务并限制非授权用户的服务,确保信息系统的业务功能能够正常运行。在这一阶段,除了保密性、完整性和可用性之外,人们还关注不可否认性需求,即信息的发送者和接收者事后都不能否认发送和接收的行为。

20世纪90年代以来,安全不再局限于信息的保护,人们需要的是对整个信息和信息系统的保护和防御,包括保护、检测、反应和恢复能力。信息保障强调信息系统整个生命周期的防御和恢复,同时安全问题的出现和解决方案也超越了纯技术范畴。信息保障阶段的典型标志是美国国家安全局制定的《信息技术保障框架》(IATF),它的核心思想是深层防御战略。

安全与应用的结合更加紧密,其相对性、动态性引起注意,追求适度风险的信息安全成为共识,安全不再单纯以功能或机制的强度作为评判指标,而是结合了应用环境和应用需求,强调安全是一种信心的度量,使信息系统的使用者确信其预期的安全目标已获满足。

1.1.3 信息安全现状及发展趋势

国际上围绕信息安全的斗争愈演愈烈,在全球信息化的同时,各种新攻击与防护技术(如对工业控制系统的攻击、无界浏览器、网络刷票、免杀等),新攻击与防护方法(如网络身份证、云安全等)层出不穷。这些新攻击与防护技术所带来的安全问题尤其突出,面对越来越严峻的安全形势,世界各国高度重视信息安全保障。信息安全已经上升到国家战略层次,国外,特别是欧美国家,其信息安全总体发展水平处于领先地位。

据Gartner分析,当前国际大型企业在信息安全领域主要有几个发展趋势。

(1) 信息安全投资从基础架构向应用系统转移。

(2) 信息安全的重心从技术向管理转移。

(3) 信息安全管理与企业风险管理、内控体系建设的结合日益紧密。

(4) 信息技术逐步向信息安全管理渗透。

结合大型企业信息安全发展趋势,国际各大咨询公司、厂商等机构纷纷提出了符合大型企业业务和信息化发展需要的信息安全体系架构模型,着力建立全面的企业信息安全体系架构,使企业的信息安全保护模式从较为单一的保护模式发展成为系统、全面的保护模式。

我国一直高度重视信息安全产业的发展,早在2003年,中共中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》,党的十六届四中全会将信息安全上升到国家安全的战略层面,明确提出"确保国家的政治安全、经济安全、文化安全和信息安全"。面对日益复杂的全球信息安全形势和国内信息安全现状,2012年,党的十八大报告中强调,要高度关注网络空间安全,并将网络空间安全、海洋安全、太空安全置于同一战略高度。2013年,党的十八届三中全会再次指出:"加大依法管理网络力度,加快完善互联网管理领导体制,确保国家网络和信息安全"。2014年,中央网络安全和信息化领导小组成立,充分体现了国家对信息安全的重视程度。国内现在以等级保护体系和分级保护体系为主要手段,以保护重点为特点,强制实施以提高对重点系统和设施的信息安全保障水平,国内的信息安全标准通过引进和消化也已经初步形成了体系。可以说,虽然目前国内的信息安全较国外有一定的距离,但也正在快速赶上。

1.1.4 ISO/OSI 安全体系结构

OSI(Open System Interconnect,开放系统互连)安全体系结构的研究始于 1982 年,当时 OSI 基本参考模型刚刚确立,其成果标志是 ISO International Organization for Standardization,国际标准化组织发布了 ISO 7498-2 标准作为 OSI 基本参考模型的新补充。1990 年,ITU 决定采用 ISO 7498-2 作为它的 X.800 推荐标准,我国的国际 GB/T 9387.2—1995《信息处理系统开放系统互连基本参考模型第 2 部分:安全体系结构》等同于 ISO/IEC 7498-2。在 ISO 7498-2 中描述了开放系统互联安全的体系结构,提出设计安全的信息系统的基础架构中应该包含 5 种安全服务(安全功能),能够对这 5 种安全服务提供支持的 8 类安全机制和普遍安全机制,以及需要进行的 5 种 OSI 安全管理方式。

1. 安全服务

OSI 安全体系结构定义了 5 种安全服务,包括鉴别服务、访问控制服务、数据完整性服务、数据机密性服务和抗抵赖性服务。

1) 鉴别服务

鉴别服务就是提供某个实体的身份保证,包括对等实体鉴别和数据源鉴别两种服务。

对等实体鉴别服务可以对两个对等实体(用户或进程)在建立连接和开始传输数据时进行身份的合法性和真实性验证,以防止非法用户的假冒和伪造连接初始化攻击。

数据源鉴别服务可对信息源点进行鉴别,确保数据是由合法用户发出,以防假冒。

2) 访问控制服务

访问控制服务是对某些明确身份的用户限制对某些资源的访问,是实现授权的一种方法。访问控制包括身份验证和权限验证,从而防止未授权用户非法访问网络资源,也防止合法用户越权访问网络资源。

3) 数据完整性服务

数据完整性服务防止非法用户对正常数据的变更,如修改、插入、延时或删除,以及在数据交换过程中的数据丢失。数据完整性服务可分为以下 5 种情形。

(1) 带恢复功能的面向连接的数据完整性。

(2) 不带恢复功能的面向连接的数据完整性。

(3) 选择字段面向连接的数据完整性。

(4) 选择自选无连接的数据完整性。

(5) 无连接的数据完整性。

4) 数据机密性服务

采用数据机密性服务的目的是保证信息的机密性。该服务提供面向连接和无连接两种数据保密方式。机密性服务还提供给用户可选字段的数据保护和信息流安全,即对可能从观察信息流就能推导出的信息提供保护。

5) 抗抵赖性服务

抗抵赖性服务可防止发送方发送数据后否认自己发送过数据,也可防止接收方接收数据后否认已经接收过数据。它由两种服务组成:一是发送(源点)非抵赖服务;二是接收(交付)非抵赖服务。这实际上是一种数字签名服务。

对付典型网络威胁的安全服务如表 1-1 所示,网络各层提供的安全服务如表 1-2 所示。

表 1-1　对付典型网络威胁的安全服务

网 络 威 胁	安 全 服 务
假冒攻击	鉴别服务
非授权侵犯	访问控制服务
窃听攻击	数据机密性服务
完整性破坏	数据完整性服务
服务否认	抗抵赖性服务
拒绝服务	鉴别服务、访问控制服务和数据完整性服务等

表 1-2　网络各层提供的安全服务

安 全 服 务		网 络 层 次						
		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			√	√			√
	数据源发鉴别			√	√			√
访问控制				√	√			
数据完整性	可恢复的连接完整性				√			√
	不可恢复的连接完整性			√	√			√
	选择字段的连接完整性							√
	无连接完整性			√	√			√
	选择字段的无连接完整性							√
数据机密性	连接机密性	√	√	√	√		√	√
	无连接机密性		√	√	√		√	√
	选择字段机密性						√	√
	业务流机密性	√		√				√
抗抵赖性	数据源发证明的抗抵赖性							√
	交付证明的抗抵赖性							√

2. 安全机制

OSI 安全体系结构没有详细说明安全服务应该如何来实现。作为指南，它给出了一系列可用来实现这些安全服务的安全机制，安全服务与安全机制的关系如表 1-3 所示。

表 1-3　安全服务与安全机制的关系

安 全 服 务		安 全 机 制							
		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	路由控制	公证
鉴别	对等实体鉴别	√	√			√			
	数据源发鉴别	√	√						
访问控制	自主访问控制			√					
	强制访问控制			√				√	

续表

安全服务		安全机制							
		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	路由控制	公证
数据完整性	可恢复连接完整性	√			√				
	不可恢复连接完整性	√			√				
	选择字段连接完整性	√			√				
	无连接完整性	√	√		√				
	选择字段无连接完整性	√	√		√				
数据机密性	连接机密性	√						√	
	无连接机密性	√							√
	选择字段机密性	√							
	业务流机密性	√					√	√	
抗抵赖性	数据源发证明抗抵赖性		√		√				√
	交付证明抗抵赖性		√		√				√

OSI 安全体系结构基本的机制有加密机制、数字签名机制、访问控制机制、数据完整性机制、认证交换机制、通信业务流填充机制、路由控制和公证机制(把数据向可信第三方注册,以便可使人相信数据的内容、来源、时间和传递过程)。

3. 安全体系结构三维图

ISO 7498-2 规定的"开放系统互连安全体系结构"给出了基于 OSI 参考模型的七层协议之上的信息安全体系结构,它定义了开放系统的 5 类安全服务,以及提供这些服务的 8 类安全机制及相应的 OSI 安全管理,并可以根据具体系统适当地配置于 OSI 模型的七层协议中。OSI 模型与安全服务、安全机制的关系如图 1-2 所示。其中,一种安全服务可以通过某种安全机制单独提供,也可以通过多种安全机制联合提供;同一种安全机制也可用于提供一种或多种安全服务。在 OSI 七层协议中,最适合配置安全服务的是物理层、网络层、传输层和应用层,其他各层都不适宜配置安全服务。

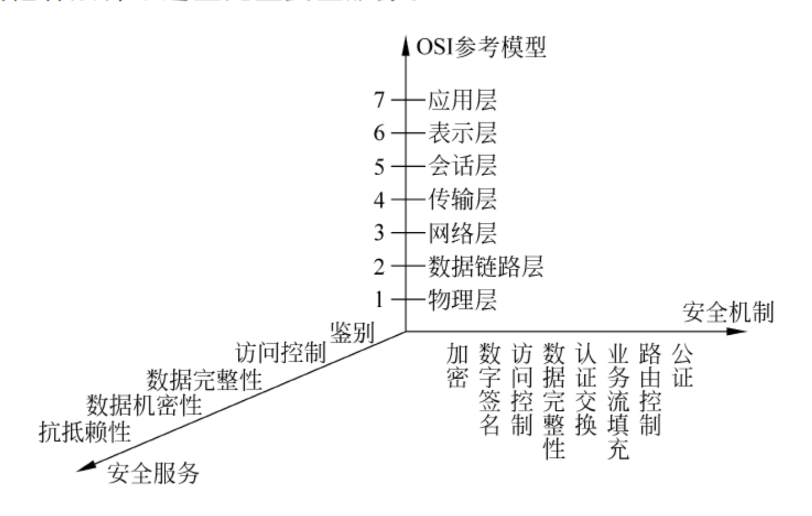


图 1-2 ISO 7498—2 安全体系结构三维图

1.2　信息安全工程的相关概念

1.2.1　信息安全工程的发展由来

可以说，信息系统安全工程是系统工程过程的基本原理在信息安全领域内的具体应用。

我国著名科学家钱学森院士认为，系统工程是组织、管理、规划、研究、设计、制造、试验和使用“系统”的科学方法，是一种对所有“系统”都具有普遍意义的科学方法。

任何系统均有其产生、发展、成熟、消亡或更新换代的过程，这个过程称为系统的生命周期。以基于系统工程的思想和方法建设信息系统为例，系统工程过程按照下述的一般方式进行。

(1) 发掘需求。

(2) 定义系统要求。

(3) 设计系统体系结构。

(4) 开展详细设计。

(5) 实现系统。

(6) 评估有效性。

在挖掘任务或业务需求阶段，主要的工程行为是描述任务/业务并考虑有关的政策要求。在定义系统功能阶段，系统工程师要明确系统的目标，定义系统背景环境，将目标转化为系统功能和性能要求，并进行功能分析，要点是分析功能之间或功能与环境之间的联系。在设计系统阶段，系统工程师要完成功能分配、概要设计和详细设计工作。在实施系统阶段，系统工程师要完成采购、建设和测试任务。最后，系统工程师要从系统是否达到了任务需求以及系统是否能够依照组织所期望的方式操作这两方面来评估系统的有效性。

可以看出，通过以上步骤完成了信息系统的建设。但该信息系统是否满足用户安全需求却得不到保障，因为安全问题的解决，不能只依靠纯粹的技术，不能靠简单的安全产品的堆砌，也不能仅靠安全管理体系建设；安全问题的解决是一个复杂的系统工程，即需要采用工程的概念、原理、技术和方法，来研究、开发、实施与维护信息系统安全。

针对信息系统安全存在的各种隐患，人们采取了一系列的安全防范措施和相应的技术，如物理隔离、防火墙、身份认证、访问控制、身份鉴别、加密、审计、监控等。但是在实际应用中，人们逐渐认识到系统安全问题涉及许多方面，不是只靠几种安全产品就能解决。

(1) 安全不是一个单一的问题。在绝大多数信息系统环境中，风险点或威胁点不是单一的，这些风险点包括物理安全、逻辑安全和安全管理三个方面。物理安全涉及关键设施设备的安全和资产存放地点的安全等内容；逻辑安全涉及访问控制和数据完整性等方面；安全管理涉及人员安全管理政策、组织安全管理政策等方面。上述任何一个方面如果出了问题，都可能引起安全事故。

(2) 安全问题是动态的。由于信息技术在不断地变化，信息技术安全问题具有动态性。今天的安全问题到明天也许不再成为安全问题，而今天无关紧要的问题，明天可能成为严重的安全威胁。这种动态性导致不可能存在一劳永逸的解决方案。

(3) 安全问题不能仅仅由技术来完全解决。由于存在着安全技术悖论，即安全产品的

安全如何保证,这个问题可以递归地问下去,因此仅仅采用安全产品来防范难以奏效。

综上所述,信息系统安全问题不仅涉及安全技术、产品等方面,还包括技术、人员、管理等多方面因素,必须采用系统化的方法加以解决。于是人们提出了用系统安全工程的思想来解决安全问题。

系统安全工程是一个非常复杂的过程,技术性和政策性都非常强。按照信息安全工程的思想来保证信息系统的安全,就要从安全体系的构成、安全基线的划分、安全风险的评估、安全策略的制定、安全工程的实施以及安全系统的管理等方面入手来解决各种问题。在这种情况下,需要有规范的方法和标准来指导系统安全的整个开发过程,于是信息安全工程应运而生。

1.2.2 信息安全工程的定义

信息安全工程是系统工程的一个子集,系统工程的原理适用于信息安全工程的开发、集成、运行、管理、维护和演变。由于信息安全工程是一门新兴学科,它的产生和发展比较晚。关于它的定义很多,并没有得到统一。但现在有一个比较全面的说法,信息安全工程是采用工程的概念、原理、技术和方法来研究、开发、实施与维护信息系统安全的过程,是将经过时间考验证明是正确的工程实践流程、管理技术和当前能够得到的最好的技术方法相结合的过程。

信息安全工程的研究范畴包括以下内容。

(1) 信息安全工程的目标、原则与范围。

(2) 信息安全风险分析与评估的方法、手段、流程。

(3) 信息安全需求分析方法。

(4) 安全策略。

(5) 安全体系结构。

(6) 安全实施领域及安全解决方案。

(7) 安全工程的实施规范。

(8) 安全工程的测试与运行。

(9) 安全意识的教育与技术培训以及应急响应技术、方法与流程。

信息安全工程建设的几个主要活动包括风险分析与评价、安全需求分析、制定安全策略、设计安全体系结构、安全工程实施及安全工程监理。其中,风险分析与评价主要是对信息系统及其处理、传输和存储信息的保密性、完整性及可用性等安全属性进行科学识别和评价。安全需求是系统设计、建设、使用、评估和监管的标准和依据,安全需求的提出应针对风险分析的结果,参照国家标准、行业标准,并遵循有关法律、法规及政府部门文件。安全策略是为发布、管理及保护敏感信息资源而制定的法律、法规及措施的综合,是对信息资源使用和管理规则的正式描述。安全策略制定者根据对信息系统风险分析的结果,结合安全目标及安全需求,提出系统的安全策略。安全体系设计一般要求设计分层、分级的安全保护体系。安全工程实施是在设计的安全体系框架的基础上,提出相应的安全服务、安全机制,以及所要采用的安全技术及产品。安全工程监理需要从工程的规范、流程、进度等方面进行监督和检查。

信息安全工程具有如下一些特性。

(1) 全面性。因为系统安全程度取决于系统最薄弱的环节,因此需要全面考虑。

(2) 过程性与周期性。信息安全工程是不断往复、不断上升的螺旋模型。

(3) 动态性。信息技术在发展,黑客水平也在提高,安全策略、安全体系、安全技术必须动态地调整,使安全系统能够跟上实际情况的变化而发挥效应。

(4) 层次性。需要用多层次的安全技术、方法与手段,分层次地化解安全风险。

(5) 相对性。安全是相对的,没有绝对安全可言。安全措施应该与保护的信息与网络系统的价值相称。实施信息安全工程要充分权衡风险威胁与防御措施的利弊与得失,在安全级别与投资代价之间应取得一个能够接受的平衡点。

(6) 继承性。在计算机以外的其他领域积累了许多从系统工程角度出发维护信息安全的方法与经验,在情况复杂的信息时代,信息安全内涵不断扩展,方法与经验不断继承与发展。

信息安全工程是信息安全保障的重要组成部分,针对目前信息化建设过程中“重技术,轻管理”“重应用,轻安全”“重要素,轻过程”“先建设,后安全”等问题,强调信息安全建设必须同信息化建设“同步规划、同步实施”,解决信息系统生命周期的“过程安全”问题。

1.3 信息安全体系模型

信息安全的建设应该立足于一个完整的安全体系。信息安全体系模型是信息安全体系建设的基础,能够为信息安全的解决方案和工程实施提供依据和参照。就像建造一座大厦需要事先设计蓝图一样,进行信息安全建设,也需要一个实施依据,这就是整体上考虑的信息安全体系。只有在整体的安全体系指导下,信息安全建设所需的技术、产品、人员和操作等才能真正发挥各自的效力。信息安全体系结构的设计并没有严格统一的标准,不同领域与不同时期,人们对信息安全的认识都不尽相同,对解决信息安全问题的侧重也有所差别。早期人们对信息安全体系的关注焦点是以防护技术为主的静态的信息安全体系。随着人们对信息安全认识的深入,其动态性和过程性的发展要求愈显重要,接下来介绍几种典型的信息安全体系模型。

1. PDR 模型

首先来看 PDR 模型,PDR 即 Protection(保护)、Detection(检测)、Response(响应)。PDR 模型是由美国国际互联网安全系统公司(ISS)提出的最早体现主动防御思想的一种网络安全模型。PDR 模型建立了一个基于时间的可证明的安全模型;定义了防护时间 Pt(黑客发起攻击时,保护系统不被攻破的时间)、检测时间 Dt(从发起攻击到检测到攻击的时间)和响应时间 Rt(从发现攻击到做出有效响应的时间),当 Pt>Dt+Rt 时,即认为系统是安全的,也就是说,如果在黑客攻破系统之前发现并阻止了黑客的行为,那么系统就是安全的。PDR 模型是一个理想模型,因为系统的 Pt、Dt、Rt 根本不可能准确定义,面对不同黑客和不同种类的攻击,这些时间都是变化的,其实还是不能有效证明一个系统是否安全。PDR 模型如图 1-3 所示。



图 1-3 PDR 模型

2. PPDR 模型

PDR 模型有很多变体，最著名的是 PPDR 模型。PPDR 模型是在 PDR 环的中间加入了 Policy(策略)，也即 PDR 循环是在策略的控制下工作的。PPDR 有时也称为 P2DR，因为引入了策略的概念，使得整个模型看起来更加的完整，并且和管理实现了衔接。PPDR 为安全问题的解决给出了一个明确的方向：提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt。PPDR 模型也存在一个明显的弱点，就是忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。PPDR 模型如图 1-4 所示。



图 1-4 PPDR 模型

3. PDRR 模型

PDRR(Protection Detection Response Recovery)模型是一个比较成熟的网络安全模型，该模型由保护、检测、响应和恢复组成了一个动态的信息安全周期，安全政策的每一部分包括一组安全单元来实现一定的安全功能。安全策略的第一部分是保护，根据系统已知的所有的安全问题做出防御措施，如打补丁、访问控制、数据加密等。安全策略的第二部分就是检测，攻击者如果穿过了防御系统，检测系统就会检测出来。这个安全战线的功能就是检测出入侵者的身份，包括攻击源、系统损失等。一旦检测出入侵，响应系统开始响应，包括事件处理和其他业务。安全策略的最后一个战线是系统恢复。在入侵事件发生后，把系统恢复到原来的状态。但 PDRR 模型侧重于技术，对诸如管理这样的因素并没有强调。PDRR 模型如图 1-5 所示。

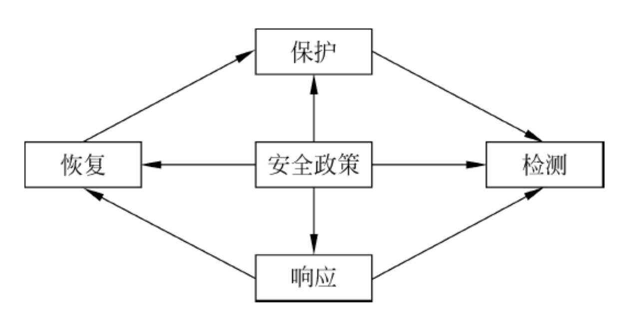


图 1-5 PDRR 模型

4. IATF 模型

当信息安全发展到信息保障阶段之后，人们越发认为，构建信息安全保障体系必须从安全的各个方面进行综合考虑，只有将技术、管理、策略、工程过程等方面紧密结合，安全保障体系才能真正成为指导安全方案设计和建设的有力依据。信息保障技术框架(Information Assurance Technical Framework，IATF)就是在这种背景下诞生的。IATF 是由美国国家安全局组织专家编写的一个全面描述信息安全保障体系的框架，它提出了信息保障时代信息基础设施的全套安全需求。IATF 创造性的地方在于它首次提出了信息保障依赖于人，操作和技术来共同实现组织职能或业务运作的思想，对技术或信息基础设施的管理也离不开这 3 个要素。尽管 IATF 提出了以人为核心的思想，但整个体系的阐述还是以技术为侧重的，对于安全管理的内容则很少涉及。它最大的缺陷在于缺乏流程化的管理要求和对业务相关性在信息安全管理体系中的体现。IATF 保障技术框架如图 1-6 所示。

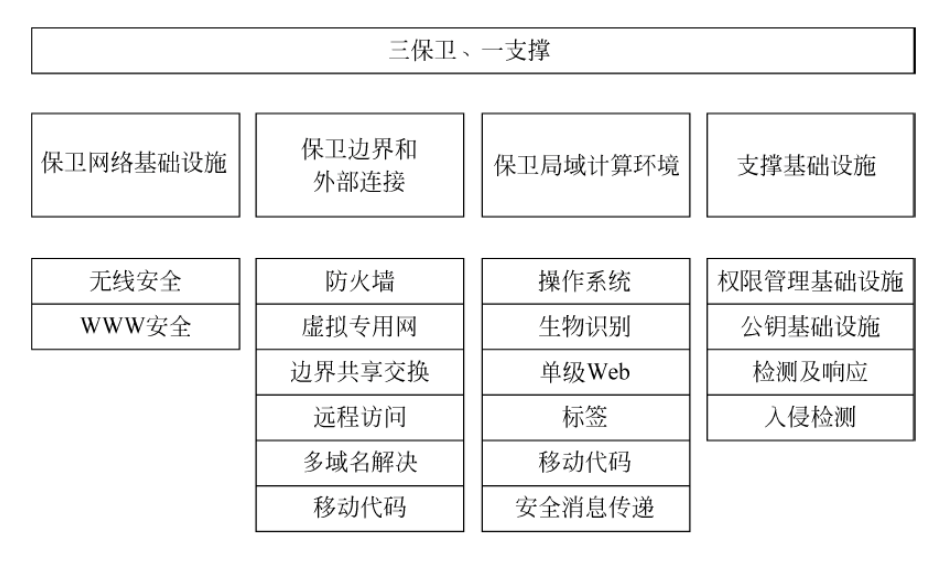


图 1-6　IATF 保障技术框架

5. WPDRRC 模型

最后来看由我国 863 信息安全专家组在 PDR 模型、P2DR 模型及 PDRR 模型的基础上提出的适合我国国情的 WPDRRC 模型，其在 PDRR 模型的前后增加了预警（Warning）和反击（Counterattack）功能。WPDRRC 模型有 6 个环节和 3 大要素。6 个环节包括预警、保护、检测、响应、恢复和反击，它们具有较强的时序性和动态性，能够较好地反映出信息系统安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。3 大要素包括人员、策略和技术，人员是核心，策略是桥梁，技术是保证，落实在 WPDRRC 6 个环节的各个方面，将安全策略变为安全现实。WPDRRC 模型如图 1-7 所示。

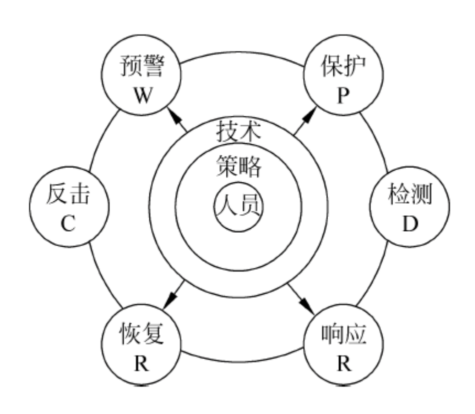


图 1-7　WPDRRC 模型

WPDRRC 模型运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的真实性、可用性、完整性、保密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

以往的一些经验教训表明，不从体系结构角度考虑信息系统的安全性、不考虑建立安全标准体系，往往会造成整体功能不完备，存在薄弱环节，部件功能重复，效率低下，评估困难，不适应需求和技术变化，相互操作困难等问题。信息安全体系模型的发展，一方面是对信息安全理解的逐渐丰富，另一方面也反映出安全技术与产品种类的日渐丰富。良好的信息安全体系模型在信息系统安全建设中起着重要的指导作用。通过模型分析，可以让人们在处理信息安全问题时全面考虑各方面的因素，避免由于遗漏一个方面而造成“短板”。

1.4 小　结

信息安全工程概念提出以来，国外已经在安全体系模型的建立及其形式化描述与分析，安全策略和机制的研究、检验以及评估系统安全性的科学方法与准则的建立等方面开展了广泛的研究，并推出了众多信息安全解决方案和产品。信息安全工程的发展，方兴未艾，有着极为广阔的研究和实践领域，人们期望它能减少信息安全相关事故，为创造一个安全的工作环境做出更大的贡献。

习　题

1. 当无法使用信息系统或信息，尤其是丧失保密性、完整性、可用性和不可否认性时，可能会带来哪些问题？
2. 什么是信息安全工程？为什么需要信息安全工程？
3. 信息安全体系模型是什么？试比较不同的信息安全体系模型。
4. 谈谈你对信息安全工程的发展的看法。

第 2 章　信息安全工程基础

本章学习目标：

- 了解并掌握系统工程相关理论基础。
- 了解并掌握质量管理相关理论基础。
- 了解并掌握项目管理相关理论基础。

2.1　系统工程基础

2.1.1　系统的定义、特征及类型

“系统”一词的出现由来已久，最早出现于古希腊莫克利特所写的《宇宙大系统》一书中，原意指事物中的共性部分和每一事物所占据的位置，即部分组成整体的意思。但直到 20 世纪 40 年代以后，“系统”一词才开始真正得到应用，并逐渐趋于完善和统一。在早期社会，人类对系统的认识比较肤浅，普遍认为系统是彼此孤立的、割裂的、互不联系的。随着科学技术的发展和长期的社会实践，人类逐渐认识到系统的含义。系统工程的研究对象，在人们的日常生活中无处不在。

(1) 银河系，太阳系，地球。

(2) 长江流域，黄土高原，珠江三角洲。

(3) 人类，中华民族，国防教育，军事通信网。

(4) 装备订货系统，航天发射系统。

(5) 三峡工程，西部大开发，振兴东北，“神舟”七号，抗击 SARS，举办奥运会等。

由于研究领域、应用对象和解决问题的不同，对系统概念的定义也不尽相同，尚未达到统一。究竟什么是系统呢？它是指逻辑上空无一物的概念，还是可以应用到工程领域的管理方法？为了避免概念的混淆所带给系统研究的困难，下面列举了国内外一些著名学者或机构的看法和观点，帮助读者理解系统的含义。

一般系统论的创始人贝塔朗菲认为“系统是相互联系、相互作用的诸元素的综合体”。他指出对于系统不能孤立地研究部分和过程，还必须研究各部分之间的相互作用，把各元素组合起来作为一个整体来考虑。

美国《韦氏大辞典》解释系统为“有组织的或是组织化了的整体，被组合的整体所形成的各种概念和原理的综合，以有规则地相互作用、相互依赖的形式组成的诸要素的集合”。

日本工业标准给出系统的定义是“许多组成要素保持有机的秩序，向同一目标的行动的集合体”。

苏联学者乌约莫夫关于系统的定义是“可以把系统定义为客体的集合，在这个集合中实现带有固定性质的关系”。

我国著名科学家、系统工程的倡导者钱学森教授认为“系统是由相互作用和相互依赖的

若干组成部分结合成的、具有特定功能的有机整体”。

上述各位学者可能对系统的定义略有不同，但是其内涵和核心思想还是一致的，他们共同指出了系统应该符合的基本条件。概括起来，所谓系统就是相互联系、相互作用的若干要素按照一定规律合成的、具有特定功能的有机整体。

根据系统的定义，可以总结出系统的一些基本特征。

1. 整体性

系统是由两个或两个以上的要素组成的整体，各个要素根据规定的任务完成既定目标，通过要素之间的协调表现出系统的整体功能。系统的整体性表述为系统整体功能不等于各组成要素之和，即“1＋1≠2”，系统的整体功能不是各组成要素的单一功能的叠加或简单的凑合，而是系统整体表现出各组成要素所没有的新功能。

“木桶原理”正是运用了系统整体性的原理，它的盛水量取决于最短木板的长度。研究任何事物都必须以事物整体为基础，脱离了整体，要素的功能和要素之间的相互作用便失去了原有的意义，从而也无法得出整体性的结论。例如，在装配汽车时，如果不对汽车零件进行组装，那么它只是一堆零散的集合，不具备任何功能，若将汽车零件根据需要组装好，它便可以发挥出汽车所特有的功能，零件的功能也通过汽车整体发挥了出来。

2. 关联性

系统内部的各组成要素之间或系统与部分之间是相互作用、相互联系的，某一要素的变化会引起其他要素的变化并且会影响系统功能的效果。例如，为了保护草原植被，政府下令禁止捕杀野狼，这是因为狼捕杀羊、野兔等食草性动物，使其数量减少，起到保护植被的作用。所谓的“牵一发而动全身”正是运用系统关联性的原理，相关性说明了要素之间相互关联的特定关系，以及这些关系之间的演变规律。

3. 目的性

系统都是为了实现某一特定目标而发挥其功能的，没有目标的系统不能作为系统工程的研究对象。为了实现既定的目标，必须赋予系统特有的功能，这也是系统之间区分的重要标志。例如，汽车的设计是帮助人们进行日常的出行，计算机的发明是帮助人们进行大规模数据的计算，电灯的发明是为了解决照明问题，它们之间由于各自功能的不同也存在差异。在设计和分析一个系统时，必须弄清楚目的，否则无法构成一个良好、有序的现实系统。例如，设计钟表的目的就是满足人们对计时功能的需要，如果人们对钟表的设计目的不清晰，则钟表的设计也就毫无意义。

4. 层次性

一般系统都具有明显的一定的层次结构。系统作为一个相互作用的诸要素总体来看，它可以分解为若干子系统，而子系统又可以分为亚子系统，以致最终分解为系统要素，这样就构成了系统空间结构的特定形式。系统的层次结构表明了不同层次子系统或要素之间的从属关系或相互作用的关系。例如一个公司就是一个层次比较明显的系统。它由子公司或二级厂、车间、工段、班组，以及相应的职能部门构成。各层次的子系统相互联系，相互作用，以其特有的功能为统一的目标而相互协调运行。

5. 环境适应性

任何一个系统都处于一定的物质环境之中，系统必须与外部环境进行物质、能量和信息

的交换，外部环境的变化也会引起系统内部因素的变化，脱离物质环境的系统不具有实际意义。因此，系统必须具有适应外界环境变化的能力才能经常以最佳的状态去实现系统的既定目标。例如，一个企业要在激烈的市场竞争中处于不败地位，就必须及时地了解市场动态、竞争对手的经营动向、产品销路、原材料供应和国家宏观政策等，企业不能适应这些变化，必然被市场淘汰，诺基亚的手机产业就是一个很好的证明，由于对市场缺乏充分的考虑，没有及时做出应变决策，导致它的手机产业无法立足。

自然界和人类社会普遍存在各种形态不同形态的系统。从不同的角度，系统可以有各种不同的种类。

1）自然系统和人造系统

自然系统是由自然物质组成的天然系统，它由自然现象发展而来，未经人类加工和制造，例如森林系统、河流系统、山脉系统、海洋系统、人类社会系统等。人造系统是为了满足人类的某些需求而有计划、有目的地设计和改造的系统，例如立体成像系统、物流系统、交通系统、医疗系统、教育系统等。

实际上，大多数系统都是自然系统和人造系统复合而成的复合系统，例如水利系统，它是在认识自然规律的基础上，通过人工作用形成的复合系统。

2）实体系统和概念系统

实体系统是由矿物、生物、机械、能量和人等实体物质组成的系统，它以研究硬件为主，属于硬科学，如机械加工、矿物资源、电力网络系统等。概念系统是由概念、原理、方法、制度等非物质实体组成的系统，它以研究软件为主，属于软科学，如法律法规系统、教育系统、军事指挥系统等。

在实际生活中，实体系统和概念系统在多数情况下是相互依赖、不可分割的，实体系统是概念系统的物质基础，概念系统为实体系统提供了指导和服务，如服务系统，既包括了提供服务的物质实体，又包括了服务方法概念子系统。

3）静态系统和动态系统

静态系统是系统的状态变量不随时间推移而变化的系统，而动态系统是系统的状态变量随时间推移而不断发生变化的系统。完全静止的系统是不存在的，模型的变量总是随时间推移而变化，静态系统可以看作动态系统的极限状态，即处于稳定状态，例如人的体温、大气压、运行的仪器设备等。

4）开放系统和封闭系统

开放系统是指与外界环境发生联系的系统，即系统与环境之间发生物质、能量、信息的交换，它具有自适应和自调节的功能，例如一个工厂、一个学校就是开放系统。反之，与外部环境隔绝或与外部环境无关的系统称为封闭系统，例如自给自足的农村、完全封闭的容器等。但是，世界上不存在绝对意义的封闭系统，任何系统都与环境有或多或少的联系，只是有时把相对独立的系统看作封闭系统。

5）确定性系统和非确定性系统

确定性系统的状态是确定的，只要确定了系统的结构和目前的状态，就可以确定将来一切时刻系统的状态。非确定性系统指的是受非确定因素影响的系统，例如随机非确定性系统、模糊非确定性系统等。

2.1.2 系统工程的概念和特点

“系统工程”这个专用名词最早在20世纪40年代由美国贝尔实验室提出，经过多年的实践，发展成为一门组织管理技术。系统工程的思想和方法可以追溯到我国古代，例如，我国四川的都江堰，是世界迄今为止年代最久、唯一留存的以无坝引水为特征的宏大水利工程。

都江堰的主体工程包括鱼嘴分水堤、飞沙堰溢洪道和宝瓶口进水口三部分，科学地解决了江水自动分流、自动排沙、控制进水流量等问题，消除了水患，使川西平原成为“天府之国”。都江堰的三个子工程融为一体，巧妙的配合实现了彻底排沙、最佳水量的自动调节。在一般人看来，都江堰的三大主体工程可能简单平常，但是它却蕴含着系统工程的思想和方法，整个工程的规划、设计和施工都十分合理。通过鱼嘴分水、宝瓶口引水、飞沙堰溢洪，形成了一个完整的“引水以灌田，分洪以减灾”的分洪灌溉系统。

系统工程是一门处于发展阶段的新兴学科，它跨越了诸多学科，并与之相互渗透、相互影响，在各个领域也都有涉及，应用范围十分广泛，这也造成人们对它的认识不一致。因此，要给出一个完善而确切的定义比较困难，下面列举一些具有代表性的定义。

美国的《科学技术辞典》对系统工程解释为“系统工程是研究复杂系统设计的科学，该系统由许多密切联系的元素所组成。设计该复杂系统时，应有明确的预定功能及目标，并协调各个元素之间及元素和整体之间的有机联系，以使系统能从总体上达到最优目标。在设计系统时，要同时考虑到参与系统活动的人的因素及其作用。”

美国著名学者H.切斯纳指出“系统工程认为虽然每个系统都是由许多不同的特殊功能部分所组成，而这些功能部分之间又存在着相互关系，但是每一个系统都是完整的整体，每一个系统都要求有一个或若干个目标。系统工程则是按照各个目标进行权衡，全面求得最优解（或满意解）的方法，并使各组成部分最大限度地互相适应。”

日本学者三浦武雄指出“系统工程与其他工程学不同之处在于它是跨越许多学科的科学，而且是填补这些学科边界空白的一种边缘学科。因为系统工程的目的是研制一个系统，而系统不仅涉及工程学的领域，还涉及社会、经济和政治等领域，所以为了适当地解决这些领域的问题，除了需要某些纵向技术以外，还要有一种技术从横向把它们组织起来，这种横向技术就是系统工程。”

我国著名科学家钱学森教授指出“系统工程是组织管理系统的规划、研究、设计、制造、试验和使用的科学方法，是一种对所有系统都具有普遍意义的方法。”

综上所述，系统工程从需求出发，为了更好地达到系统的目标，对系统组成要素、组织结构、信息流、控制机构等进行分析研究的科学方法。它运用组织管理技术，使系统的整体与局部之间的关系协调和相互配合，实现总体最优化运行。

从以上列举的定义中可以看出系统工程有以下几个特点。

（1）系统工程以规模庞大、结构复杂的系统为研究对象。

（2）系统工程跨越诸多学科，涉及多个领域的知识，是一门基于多学科理论的新兴边缘学科。

（3）在处理规模庞大、结构复杂的系统时，需要采用定性和定量分析相结合的方法。

2.1.3　系统工程的形成与发展

系统工程起源于 20 世纪 40 年代，到 60 年代形成体系，大致经历萌芽、发展和初步成熟三个时期。

1. 萌芽时期

第一次世界大战期间，出现了应用于军事运筹学的雏形。20 世纪初，美国“管理之父”泰勒创造了科学管理方法体系，研究了合理工序和工人活动的关系，探索了管理的规律，到 20 年代逐步转变为工业工程，主要研究生产在时间和空间上的管理技术。20 世纪 40 年代，美国贝尔实验室的 E. C. 莫利纳和丹麦哥本哈根电话公司的 A. K. 爱尔朗提出了“系统工程”这一专用名词，他们在研制电话自动交换机时，意识到不能只注意电话机和交换台设备技术的研究，还需从通信网络的总体上进行研究。他们把研制工作分为规划、研究、开发、应用和通用工程五个阶段，此后又提出了排队论原理，并应用到电话通信网络系统中，推动了电话事业的飞速发展。

第二次世界大战期间，由于战争的需要，军事运筹学得到快速发展。运筹学的发展为早期系统工程的萌芽奠定了理论基础。1940—1945 年，美国在研制原子弹的“曼哈顿”计划中，运用了系统工程的方法进行协调，在较短的时间内取得了显著成效。后来，这种理论也被推广到经济管理领域和工业生产领域，扩大了系统工程的应用范围。1945 年，美国建立了兰德公司，结合数学方法和工程方法开发出了“系统分析”方法，在美国国家发展战略、国防系统开发、宇宙空间技术以及经济建设领域的重大决策中，发挥了重要作用。20 世纪 40 年代后期，随着信息论、控制论的诞生和广泛应用，以及世界第一台电子计算机的发明，系统工程的雏形开始出现。

2. 发展时期

系统工程教育开始于 20 世纪 50 年代，美国理工学院开设了“系统工程”的相关专业课，培养学生运用系统工程方法对系统进行管理，创造性地解决问题。1957 年，美国的古德和麦克霍尔合作出版了第一本以“系统工程”命名的著作——《系统工程》。此后，“系统工程”作为专业术语沿用至今。1958 年，美国海军特别计划局在执行“北极星”导弹核潜艇计划中发展了控制工程进度的新方法——计划评审技术（Performance Evaluation Review Technique，PERT），采用这种技术使研制任务提前两年完成，系统工程学也被引进到管理领域。1962 年，A. D. 霍尔编写的《系统工程方法论》阐述了作者长期从事通信系统工程的成果，内容涉及系统环境、系统要素、系统理论、系统技术、系统数学等方面。同年，美国国防部长麦克马拉提出了 PPBS 系统（即规划、计划、预算系统），该系统有效地解决了海陆空三军的资金预算问题，在节约经费方面取得了巨大的成就。1963 年，美国亚利桑那大学成立了系统工程系，其他一些院校也纷纷设立了系统工程的课程或研究中心。1964 年起，美国每年都举行系统工程年会，出版刊物，并设立了工程学位。这时，系统工程已开始成为一门独立的学科。

3. 初步成熟时期

1965 年，麦克霍尔编写了《系统工程手册》，书中包含了比较完整的系统理论、系统方法、系统环境、系统部件、系统技术以及一些数学基础等内容。该书的编写标志着系统工程

初步形成了一个较为完整的理论体系。

1969 年,“阿波罗”宇宙飞船登月计划成功。“阿波罗”计划是一项举世瞩目的复杂庞大的工程计划,它的全部任务由地面、空间和登月三个部分组成。“阿波罗”飞船和“土星五号”运载火箭,由 860 多万个零件构成,有众多的子系统,各个子系统之间纵横交错,相互联系,相互制约。在规划和实施这项计划时,由于运用了系统工程学的理论和方法,提前两年将三名宇航员送到月球。“阿波罗”登月计划的实施,是典型运用系统工程这种组织管理技术取得显著效果的典型事例,这也标志着系统工程学可以结合工业生产使用,并取得辉煌的成就。

进入 20 世纪 70 年代,无论从理论来讲还是从技术方面来看,系统工程都日趋完善和成熟,系统工程的应用领域也在继续向社会、经济、生态等方面扩展,打破了传统的系统工程的概念,真正推广到所有领域。目前,多所高校纷纷开设了“系统工程”课程,培养了大量的系统工程师、系统分析师和系统科学家。系统工程已发展到解决复杂系统的最优化阶段,它几乎涉及各个领域,从社会科学到自然科学,从经济基础到上层建筑,从城市规划到生态环境,从生物科学到军事科学,无不涉及系统工程,无不需要系统工程。

2.1.4 系统工程的方法与步骤

在系统工程的长期实践中,逐渐形成了一套科学的工作方法和步骤。由于系统工程跨越诸多学科,涉及多个领域,每个学科又有自身的特点和方法论,要在不同的系统对象上套用同一种模式显然是不现实的。因此,系统工程的方法与步骤只是处理问题的一般方法与步骤,是一种基于原则的系统思考过程。按照这个方法与步骤,对一般系统很容易了解,对于结构复杂的系统,也不会显得无从下手。在实际应用过程中,系统一般遵循这一原则,但是由于研究对象的不同,所采用的方法和步骤也会不同,所以对于具体问题,只能根据系统思想的基本原则、立场和观点,灵活地运用。

系统工程思考问题和处理问题的方法,一般称为系统方法。系统工程的方法体系是不同方法的有机组合,具备了各种方法的特点。这种方法的实质是运用系统思想和各种数学方法以及电子计算机工具来实现系统的模型化和最优化,以此进行系统分析和系统设计。为了更好地处理系统工程的问题,不仅需要在了解各学科的基础上学习各种系统工程的基本方法,还要在实际应用中掌握这些方法与步骤,获取经验。

20 世纪 60 年代,许多学者对系统工程的方法进行了积累和总结,其中,具有一定代表性的方法主要是美国贝尔实验室的霍尔所提出的霍尔三维结构,如图 2-1 所示。霍尔将系统工程的工作步骤和阶段、各阶段的思维过程、各个思维过程涉及的知识概括为时间维、逻辑维和知识维。

三维结构的时间维表示系统工作的各个阶段,一般分为 7 个阶段。

(1) 规划阶段。对系统进行调研,明确系统目标,提出规划。

(2) 拟订方案。根据具体的问题提出切实可行的计划方案。

(3) 研制阶段。做出研制方案及生产计划。

(4) 生产阶段。按计划生产出系统零部件以及整个系统,提出安装计划。

(5) 安装阶段。按照安装计划安装系统,并完成系统的运行计划。

(6) 运行阶段。将系统按照预定的功能运行。

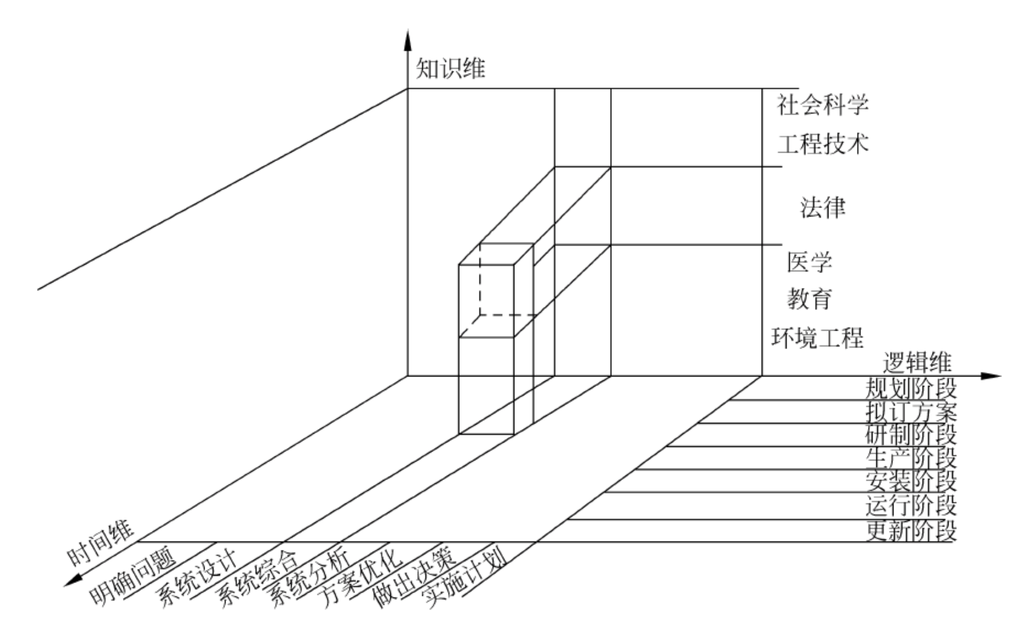


图 2-1　霍尔三维结构

(7) 更新阶段。改进旧系统或取消新系统，使之更加有效地工作。

三维结构的逻辑维表示时间维的每一个阶段内所要进行的工作和遵循的思维过程，分为 7 个阶段。

(1) 明确问题。弄清楚研究的是什么性质的问题，以便设定解决方案。

(2) 系统设计。提出所解决问题希望达到的目标，并制定评价系统功能的指标体系。

(3) 系统综合。提出并形成系统的可行方案，方案明确系统的参数和结构。

(4) 系统分析。建立模型，将这些方案与评价指标联系起来推断出各种可能性结构。

(5) 方案优化。基于系统模型，优化方案参数，尽可能满足系统的评价指标最优。

(6) 做出决策。根据方案优化的结果，选出最佳方案。

(7) 实施计划。根据决策的结果，拟订具体的实施计划，并组织实施。

三维结构的知识维表示逻辑维的每个思维过程所需要的各种专业知识和技术知识。霍尔把这些知识分为社会科学、工程技术、法律、医学、教育和环境工程等。钱学森教授认为“系统工程的理论基础，除了共同性的基础之外，每门系统工程又有各自的专业基础。这是因为对象不同，当然要掌握不同对象本身的规律。例如工程系统工程要靠工程设计，军事系统工程要靠军事科学等”。

2.2　质量管理基础

2.2.1　质量概述

质量是质量管理的研究对象，是事物的本质特性之一。质量正面临着越来越严峻的挑战，由于未能严格把关，导致许多产品出现质量问题，例如三星手机爆炸、丰田召回门、双汇瘦肉精等事件层出不穷，如何保证产品质量已成为现代工业社会和各国经济建设中一个受到普遍关注的突出问题。无论是发达国家还是发展中国家，都深刻感受到提高质量的紧迫

感和不提高质量就不能生存的危机感。但是对于到底什么是质量,如何提高质量,每个人的看法可能不同,采用的方法和手段也很有限,导致生产的产品和工作质量总存在这样或那样的不如意。

质量总是与人们的生活息息相关,没有人否认质量。例如,食品、药品的质量关系到人们的健康与安全;家用电器的质量关系到使用的舒适度和便捷性;乘坐的交通工具的质量关系到了人们的日常出行……每个人都期望自己使用的产品都有满意的质量,但往往不能如愿以偿。产品质量的优劣直接关系着现实生活中人们的生活状况,必须认真对待。例如,1985年,海尔生产的第一批冰箱不合格,张瑞敏就坚决把有毛病的76台冰箱都砸掉了。通过这件事,海尔全员意识到了质量的重要性,在1988年12月海尔就得到了全国同行业的第一块金牌,海尔的员工也因此树立了严格的质量观。海尔在经营生产中始终向员工反复强调:用户是企业的衣食父母。在生产经营过程中,海尔坚持"精细化,零缺陷",让每个员工都明白"下道工序就是用户"。这些思想被员工自觉落实到行动上,每个员工将质量隐患消除在岗位上,从而产品合格率始终保持100%,这也奠定了海尔在电器领域的龙头地位。只有提高质量,才会给企业带来竞争力和生命力,才能保障企业的生存与发展。

在相当长的一段时间,人们对"质量"的概念非常模糊,总是将质量与奢华混为一谈,例如,豪华的大房子,昂贵的汽车,各种名牌、奢侈品,但是如果顾客只是需要居住舒适的房子、日常出行简单方便、生活无忧无虑,那么奢华的东西就体现不出它们的价值。在质量的内容不断充实、完善和深化的阶段,人们对质量的认识也经历了一个不断发展和完善的过程。

美国质量管理专家克劳斯比从生产者的角度出发,把质量概括为"产品符合规定要求的程度,而不是好","好、优秀、独特"等术语都是主观的和模糊的。只有所有标准都给予定义和衡量,质量的衡量才是可能的和有实际意义的。例如,一辆符合所有设计规格的小汽车就是"有质量"的汽车。

美国质量管理专家朱兰博士认为,质量应该从用户的角度出发,即产品在使用时能够成功满足用户需要的程度。用户对产品的基本要求就是适用,适用性恰如其分地表达了质量的内涵。例如,用户要求手机可以上网、聊天、视频等,对智能手机的使用需求就要比非智能手机的大。

ISO 8402定义质量是"反映实体满足明确和隐含需要能力的特性总和"。从定义来看,质量就其本质来说是一种客观事物具有某种能力的属性,满足人们的需要,需要有两个层次构成:第一个是产品的符合性;第二个是产品的适用性。

ISO9000—2000把质量定义为一组固有特性满足要求的程度。在这个定义中,固有特性是事物本来就有的,例如外观、功能、适应性、安全性等。质量以顾客满意为衡量依据,满足顾客明示的、隐含的需要和期望。不同产品的固有特性和赋予特性不同,某种产品的赋予特性可能是另一种产品的固有特性。例如,供货及时性是汽运公司工作的固有特性,但对制造部门来说则是赋予特性。

20世纪90年代,摩托罗拉、通用电气等企业先后推行6σ管理,逐步确定了全新的卓越质量理念:顾客对质量的感知远远超出其期望,质量意味着没有缺陷。根据卓越质量的理念,体现顾客价值、追求顾客满意和顾客忠诚、降低资源成本、减少差错和缺陷、降低和抵御风险等成为质量衡量的依据。

质量的定义经历了符合性质量、适用性质量,再到满足性质量、卓越质量的演变,至今质

量的概念仍然随着经济和社会的发展在不断地发展。质量是一个发展的概念，其最终判决权在顾客和相关方那里，它的本质含义是经济学的，即以最低的成本获取最大利益。

从质量的定义可以了解到，质量具有经济性、广义性、时效性和相对性。

1. 经济性

实现高质量是需要付出代价的。一般来说，要求越高，质量的成本就会越高。虽然组织和顾客从不同的角度关注质量，但是价廉物美是人们的价值取向，物有所值就是表明质量具有经济性的特征。顾客和组织对经济性的考虑是一样的。

2. 广义性

质量不仅指产品质量，也指过程和体系的质量。

3. 时效性

质量的高低是和要求紧密联系的，由于顾客的要求和期望是不断变化的，组织就需要不断调整对质量的要求。要求的变化也就体现了质量判定标准的变化。随着时间的推移，过去被认为是合格的产品，现在可能被判定为不合格产品。

4. 相对性

顾客可能对同一产品的同一功能提出不同的需求，也可能对同一产品的不同功能提出不同的需求。需求不同，质量要求也不同，只有满足需求的产品，才被判定为质量好的产品。

2.2.2 质量管理概述

在谈到质量管理时，先考虑一个问题：人们在购买商品时为什么倾向于名牌产品？大多数人认为它们可以为我们提供满意的产品，那么为什么它们可以提供令我们满意的产品呢？因为它们大吗？历史悠久吗？贵吗？其实最重要的是它们有一套以零缺陷为目标的不断改进的、科学的、严格的质量控制方法来保证不向顾客交付有缺陷的产品和服务。

技术和管理是国民经济系统中两个相互独立又相互依存的组成部分，技术很重要，管理更重要，所谓“三分技术，七分管理”就是一个形象的说明。质量管理是企业管理的一个重要组成部分，它的主要研究对象是产品质量的产生、形成和实现过程的管理。随着生产和科学技术的不断发展以及管理科学化、现代化的要求，质量管理在整个企业管理中的地位和作用越来越显得重要；同时有关对质量管理的理论、技术和方法的探索，也越来越丰富和深化。目前，质量管理已经从管理科学中分离出来，形成了一门新兴的“边缘学科”。

质量管理影响着人们的工作和生活，关系着千千万万户家庭的舒适和安全，牵动着人们的切身利益。缺乏质量管理的工程得不到保证，质量管理就像是人们赖以生存的大堤，一旦“大堤”崩塌，那么人们的安全和利益将失去保障。2003年2月1日，美国“哥伦比亚”号航天飞机在着陆前爆炸，7名宇航员全部遇难，顿时引起了整个世界的震惊，美国航天负责人也因此辞职，美国航天事业受到重创。事后调查发现，造成此灾难的凶手竟是一块脱落的隔热瓦，这令许多人意想不到，“哥伦比亚”号航天飞机有两万多块隔热瓦，能抵御3000℃高温，避免航天飞机返回大气层时外壳被融化。航天飞机是高科技产品，许多标准是一流的，质量把关也是很严格的，但就一块脱落的隔热瓦，0.5%的差错葬送了价值连城的航天飞机，还有无法用价值衡量的宝贵的7条生命。由这个案例可以看出质量管理在人们日常生活的重要性，一旦质量管理出了问题，人们的生命安全也会受到威胁。

ISO 8042 将质量管理定义为：确定质量方针、目标和职责，并在质量体系中通过诸如质量计划、质量控制、质量保证和质量改进等手段来实施的全部管理职能的所有活动。

美国质量管理大师朱兰对质量管理的基本定义：质量就是适用性的管理，市场化的管理。

费根堡姆的定义：质量管理是"为了能够在最经济的水平上并考虑到充分满足顾客需求的条件下进行市场研究、设计、制造和售后服务，把企业内各部门的研制质量、维持质量和提高质量的活动构成为一体的一种有效的体系"。

ISO 9000—2000 定义质量管理是"在质量方面指挥和控制组织的协调的活动"。这些"活动"包括制定质量方针和质量目标、质量策划、质量控制、质量保证、质量改进。

1. 质量方针和质量目标

质量方针是由组织的最高管理者正式颁布的该组织的总质量宗旨和方向。质量方针是企业经营总方针的组成部分，企业各部门和全体人员执行质量职能和从事质量活动时必须遵守和依存的行动纲领。不同的企业具有不同的质量方针，但都必须具备明确的号召力。企业管理者将质量方针的关键信息和关键词语形成文件进行宣传。

质量目标是组织在质量方面所追求的目的，是对质量方针的展开和具体实现。目标既要体现先进性又要体现可行性，便于实施和检查。

2. 质量策划

质量策划致力于制定质量目标并规定必要的作业过程和相关资源的分配，以实现质量目标。质量策划是指导与质量有关的活动，即指导质量控制、质量保证和质量改进的活动，关键在于质量目标的设定和实现。在质量管理中，质量策划的地位低于质量方针的建立，是设定质量目标的前提，高于质量控制、质量保证和质量改进。质量控制、质量保证和质量改进只有经过质量策划，才能确定质量目标和对象，才能采取有效的措施和方法。因此，质量策划是质量管理诸多活动中不可或缺的中间环节，是连接质量方针和具体的质量管理活动之间的桥梁和纽带。

3. 质量控制

质量控制是指为满足质量要求所采取的作业技术和活动。在产品生产过程中，质量控制监视着质量形成过程，消除质量环上所有阶段引起不合格或不满意效果的因素，使产品向着预定的目标发展，以达到质量要求，获取经济效益，而采用的各种质量作业技术和活动。

作为质量管理的一部分，质量控制适用于组织对任何质量的控制，它不仅仅局限于生产领域，在产品的设计、生产原料的采购、服务的提供、市场营销人力资源的配置等领域都发挥了重要作用。质量控制是为了使产品或服务达到质量要求而采取的技术措施和管理措施方面的活动，其目标在于确保产品或服务质量能满足要求。

4. 质量保证

质量保证的关键在于信任—对达到预期质量要求的能力应提供足够的信任。质量保证在订货之前就已建立好，如果缺乏这种信任，顾客与供方也不会达成交易。质量保证是为使人们确信产品或服务能满足质量要求而在质量管理体系中实施并根据需要进行证实的全部有计划和有系统的活动。质量保证以保证质量、满足要求为基础和前提，其主要目的是使用户确信产品或服务能满足规定的质量要求。

质量保证不是单纯的保证质量，保证质量是质量控制的任务，质量保证的工作是加强质量管理、完善质量管理体系、完善质量控制，以便准备好客观证据，并根据对方的要求有计划、有步骤地开展提供证据的活动。

5. 质量改进

质量改进是为向本组织及其顾客提供增值效益，在整个组织范围内所采取的提高活动和过程的效果与效率的措施。作为质量管理体系的一部分，质量改进是一个经常性、有效地提高质量的活动，关键在于消除系统性的问题，对现有的质量水平在控制的基础上加以提高，使质量达到一个新水平、新高度。

质量改进致力于增强满足质量要求的能力，其目的是为了向组织的受益者提供更多的收益，所采取的提高质量过程效益和效率的各种措施。当然，质量改进必须按照一定的科学过程进行，其基本过程是 PDCA（Plan Do Check Action）循环，即计划、实施、检查和处理四个阶段，它具体内容如下。

（1）制定方针、目标、计划书、管理项目等。

（2）按照计划实施具体对策。

（3）实施了具体对策后，验证其结果。

（4）总结成功的经验，实施标准化，以后可以按照该标准进行生产。

对于没有解决的问题由下一轮的 PDCA 循环处理，为下一轮 PDCA 提供材料。

2.2.3　质量管理的发展历程

20 世纪 40 年代，质量管理作为一门新兴学科开始发展和深化，其发展的历史并不太长。质量管理是由商品竞争的需要和科学技术的发展而产生、形成、发展至今的，是同科学技术、生产力水平以及管理科学化和现代化的发展密不可分的。作为一门新兴学科，它是社会化大生产的产物，也是生产力发展的必然结果。

从质量管理的发展历史看，不同时期质量管理的理论、技术和方法都在不断地发展和变化，并且有不同的特点。从实践看，按照解决质量所依据的手段和方式来划分，质量管理发展至今的全过程，可分为质量检验、统计质量控制和全面质量管理三个阶段。

1. 质量检验阶段

20 世纪初，人们普遍对质量管理的认识仅限于对产品质量的检验，通过严格检验来保证出场或转入下一道工序的产品质量。因此，质量检验工作就成了这一阶段执行质量职能的主要内容。质量检验所使用的手段是各种各样的设备和仪表，方式是严格把关，对零件和产品进行百分之百的检验。在由谁来执行这种质量职能的问题上，在实践中也有一个逐步变化的过程。

在 20 世纪以前，产品的生产和质量检验全部由手工操作者进行控制和把关，工人既是生产者，又是检验者。因此，操作者自我控制的管理称为操作者的质量管理。

1918 年，美国工程师泰勒根据 18 世纪产业革命以来工业生产管理的实践经验，提出了“科学管理”理论，主张在人员中科学分工，实现计划职能和执行职能相分开，一部分人负责设计、计划，另一部分人负责执行。该理论强调了工长在保证质量方面的作用，在工厂中设立了专职检验的职能工长。这样，执行质量检验的责任就由操作者转移给工长。因此，可以

称为工长的质量管理。

1940 年前后，由于企业规模的扩大，带来了生产规模和生产批量的不断扩大，大多数企业都设置了专职的检验部门，由直属厂长直接负责全厂各个生产单位的产品检验工作，这种质量检验的职能又由工长转移给了专职的质量检验人员。因此，可以称为检验员的质量管理。专职检验的特点是“三权分立”，即有人专职制定标准；有人负责生产制造；有人专职按照标准检验产品质量。专职就是从生产成品中挑出废品，保证出厂产品质量，又是一道重要的生产工序。通过检验，反馈质量信息，从而预防今后出现同类废品。但同时又应看到，这种检验也有其弱点：第一，是出现质量问题容易扯皮、推诿，缺乏系统优化的观念；第二，它属于“事后检验”，无法在生产过程中完全起到预防、控制的作用，一经发现废品，就是“既成事实”，一般很难补救；第三，它要求对成品进行百分之百的检验，这样做有时在经济上并不合理（增加检验费用，延误出厂交货期限），有时从技术上考虑也不可能（例如破坏性检验），在生产规模扩大和大批量生产的情况下，这个弱点尤为突出。

2. 统计质量控制阶段

随着工业化的发展和产量的提高，检验人员随之增加，人数最多的时候约占到公司的 30%，对产品的成本也造成了很大的压力。后期检验中，质量不合格的产品也出现了，产品的生产成本被迫提高了。在大批量生产的情况下，事后检验信息由于不能及时反馈给公司而造成了巨大的损失，而且采取人力检验的方式成本太高，这就要求用更经济的方式来解决质量检验问题，并要求事先预防成批废品的产生。在质量检验阶段时，一些著名的统计学家和质量管理专家就开始注意质量检验的弱点，并设法运用数理统计方法去解决这些问题。

统计质量控制是用管理统计的方法控制整个生产过程的质量，该阶段的主要特点是应用数理统计原理和抽样技术对生产过程进行控制，以预防不良质量产品的出现，即进行事前的、预防性的生产过程控制。质量管理从“事后把关”的阶段发展到了“事先预防”的阶段，开创了质量管理的新局面。

统计质量控制阶段的开始时间一般认为是 20 世纪 40 年代至 50 年代末，正式在工业生产中推广应用是从第二次世界大战开始的。第二次世界大战开始后，由于军需品面临严重问题，质量检验的弱点暴露无遗，检验部门成为生产过程中最薄弱的环节。由于事先无法控制生产过程中的质量状况，检验的工作量大，致使军需品的生产经常不能按期交货，严重影响前线的军需供应。为克服这一影响，美国政府开始推广运用统计质量控制方法，用数理统计方法制定了战时质量管理标准。美国军政部门随即组织一批专家和工程技术人员，于 1941—1942 年间先后制定并公布了《质量管理指南》《数据分析用控制图》《生产过程中质量管理控制图法》，成功解决了武器等军需品的质量问题，使美国军工生产在数量上、质量上和经济上都占据世界领先地位。由于采用了统计质量控制方法，这给这些军工企业带来了巨额利润。战后，其他企业也竞相仿效。质量统计控制方法成为质量管理的主要内容。

统计质量控制强调对生产制造过程的预防性控制，使质量管理由单纯依靠质量检验事后把关，发展到突出质量的预防性控制与事后检验相结合的工序管理，成为进行生产过程控制强有力的工具。但由于统计质量管理过分强调统计方法，忽略了组织管理和生产者能动性，致使人们误认为“质量管理好像就是数理统计方法”“质量管理是少数数学家和学者的事情”。这些影响了质量管理方法的普及，限制了它的发展。

3. 全面质量管理阶段

进入 20 世纪 50 年代之后，随着社会生产力的迅速发展，科学技术日新月异，工业生产技术手段越来越现代化，工业产品更新换代也越来越频繁。

美国的“阿波罗”飞船零件有 560 万个，如果零件的可靠性只有 99.9%，则飞行中就可能有 5600 个机件要发生故障，后果不堪设想。为此，全套装置的可靠性要求在 99.9999%，在 100 万次动作中，只允许失灵一次，连续安全工作时间要在 1 亿～10 亿小时。如此要求，单靠统计方法控制是不够的，还需要一系列的组织管理工作，要对设计、准备、制造、销售和使用等环节都进行质量管理，统计方法只是其中的一种工具。这样，新的历史条件和经济形势对质量管理提出了新的要求，使质量管理从 SQC 向更高级的全面管理发展。

最早提出全面质量管理概念的是美国通用电气公司质量经理阿曼德・费根堡姆。1961 年，他出版了一本著作《全面质量管理》。该书强调执行质量职能是公司全体人员的责任，他提出：“全面质量管理是为了能够在最经济的水平上并考虑到充分满足用户要求的条件下进行市场研究、设计、生产和服务，把企业各部门的研制质量、维持质量和提高质量活动构成为一体的有效体系。”全面质量管理，就是对产品实行总体的、综合的管理，并在企业中建立一套完整的质量管理体系，以便生产出可满足用户要求的优质产品。全面质量管理源于美国，但首先在日本取得巨大成效。由于全面质量管理符合当时世界经济技术发展的需要，所以很快普及到各工业发达国家，我国在 1978 年开始先后在各行业推行。全面质量管理从 20 世纪 60 年代发展至今，其内容和方法日趋完善，并形成了完整的科学体系。通常称全面质量管理阶段是质量管理的完善期和巩固期。

应该看到，质量管理发展的三个阶段不是孤立的，前一个阶段是后一个阶段的基础，后一个阶段是前一个阶段的继承和发展。

2.2.4　质量管理的原则

1. 以顾客为关注焦点

组织依存于顾客。因此，组织应当理解顾客当前和未来的需求，满足顾客的要求并争取超越顾客的期望。

2. 领导作用

领导者应当建立组织统一的宗旨和方向，并创造和保持使员工能够充分参与和实现组织目标的内部环境。

3. 全员参与

各级人员是组织之本，只有全员的充分参与，才能使他们的才干为组织带来效益。

4. 过程方法

将活动和相关的资源作为过程进行管理，可以更高效地得到期望的结果。

5. 管理的系统方法

将相互关联的过程作为系统加以识别、理解和管理，有助于组织提高实现目标的效率和有效性。

6. 持续改进

持续改进整体业绩应当是组织的一个永恒目标。

7. 基于事实的决策方法

有效的决策是建立在数据和信息分析基础上的。

8. 互利的供方关系

组织与供方是相互依存的,互利的供方关系可以增强双方创造价值的能力。

八项管理原则系统地阐述了企业建立质量管理体系,按照 ISO 9000 标准进行管理理念、管理目标、管理基础、管理方法和相关方关系处理。标准提出以顾客为中心,让顾客满意的理念,指出一切工作应该以持续改进为目标,在领导的作用和全员参与的基础上,采用过程方法、管理的系统方法和基于事实决策的方法进行管理,本着互惠互利的原则处理供方关系。

2.3 项目管理基础

2.3.1 项目的定义、特征及分类

首先看看现实生活中发生的一些事例。

某大学承担国家研究课题,研究生产治疗非典型肺炎的药物,希望在 5 年内出成果,该研究项目同时也得到一些药厂的资助;某企业为了满足市场的需要,准备扩大生产规模,新建设一条世界一流的生产线,这个项目将历时一年,投资 5000 万元……

类似这样的事例在人们的日常生活中随处可见,大到长江三峡水利枢纽工程、阿波罗二号登月计划、奥林匹克运动会、人造卫星等,小到手机的生产、汽车的制造、工厂的建设、新药物的研发等,诸如这些都可以称之为项目。在当今社会,项目已涉及人们生活的方方面面,可以说项目无处不在。

在上述事例中,由于项目在不同的领域,因此项目的内容可以说是千差万别,那么,项目的科学含义究竟是什么?人们又是如何理解项目的呢?

质量管理大师朱兰提出,一个项目就是一个计划要解决的问题。该定义认为,项目开始的前提是在有计划的基础上,目的是解决问题。

美国项目管理权威机构——项目管理协会(Project Management Institute,PMI)认为,项目是一种被承办的旨在创造某种独特产品或服务的一次性努力。

R. J. 格雷厄姆认为,项目是为了达到特定目标而调集到一起的资源组合,它与常规任务之间关键的区别是:项目通常只做一次;项目是一项独特的工作努力,即按某种规范及应用标准导入或生产某种新产品或某项新服务。这种工作努力应当在限定的时间、成本费用、人力资源等项目参数内完成。

国际化标准组织从项目管理过程的角度对项目给出的定义是:项目是由一系列具有开始和结束日期、相互协调和控制的活动组成的,通过实施活动而达到满足时间、费用和资源等约束条件和实现项目目标的独特过程。

尽管从不同的角度出发,对项目的描述不尽相同,但是去掉具体内容,它们的共同特征

是可循的。一般项目特征可归纳为以下几点。

1. 临时性

每一个项目都有明确的开始时间和结束时间，没有可以完全照搬的先例，它是一次性的、不可重复的，例如，建造空间站就是独一无二的，之前从来没有过尝试。项目从整体来说，任务完成或由于某种原因无法继续进行下去时，项目就结束。例如，建立一个核电站可以视为一个项目，当核电站建成投入使用后，也就意味着项目的结束。

项目的临时性也决定了项目组织的临时性，项目组织一般是为某一特定的项目而组建的，项目结束也标志着项目组织的解散。

2. 独特性

项目是为创建某一独特的产品、服务或成果而临时进行的一次性努力，在某些方面它会有明显的特点，不会有同样的现象。

每个项目都是独特的，由于它有区别于其他任务的特殊要求，或者名称相同，内容不同；或者内容相同，然而时间和地点，内部和外部的环境、自然和社会条件与其他项目不同，例如，在以同样的建筑风格和施工方案来建造两个商城时，尽管两个商城看上去一模一样，但是两个商城会因不同的施工时间、施工地点和不同的管理方式，依然具有自己的独特本质。

3. 制约性

项目的制约性是指每个项目都在一定程度上受到客观条件和资源的限制。在项目实施时，项目需要运用各种资源来进行，除了受到时间限制外，它还受到资金、人力资源、技术和信息资源的限制，这些限制条件和项目所处的环境的一些约束因素构成了项目的制约性。如果项目在人力、物力、财力、时间等方面的资源宽裕，制约性小，那么其成功的可能性就会高；相反，则项目成功的可能性就会大大降低。例如，10 个人在 3 天内完成 100 个摄像头的安装与调试，“10 个人”“3 天内”“100 个摄像头”“完成安装与调试”均属于约束条件。

4. 渐进明细性

渐进明细性即人们常说的“不确定性”。项目在执行过程中包含着一定的不确定性。在一个项目开始前，只能粗略地定义和描述，随着项目的进展，这些目标和过程逐渐清晰、明朗、完善和精准。渐进明细也暗示着在项目进展中，一定会出现修改、纠正、补充、删除等现象，发生相应的变更。例如在一个软件开发项目中，由于在前期客户的需求不明确，开发团队只能建立一个快速原型模型，然后用户在了解模型后提出修改意见，开发团队不断在原型上进行修改，这要求项目经理在实施项目时，正确面对，不要惊慌。

5. 目的性

项目的目的性是指任何一个项目必须具有详细而明确的目标，即在实施项目时所要达到的期望结果。时间目标上，项目在规定的时间段内完成；成果目标上，在时间期限内提供某种规定的产品、服务或其他成果。项目的一切工作是以目标为导向，目标贯穿于项目始终，项目计划和一系列实施活动都是围绕目标而展开的。项目的目标依照项目范围、进度计划和质量、成本来定义，使之明确或量化。

6. 周期性

项目的周期性是指项目往往有一个明确的开始日期和实现目标的结束日期。例如，三

峡工程分三期，从 1994 年开工，到 2009 年竣工，总工期 16 年。项目有具体的时间计划和有限寿命，项目目标的完成意味着项目的结束，没完没了或重复性的工作不能称为项目。

按照不同的标准和原则，项目可以进行不同的分类，如表 2-1 所示。

表 2-1 项目分类

分类标准	分类内容
按照规模大小划分	特大型项目、大型项目、中型项目、小型项目
按照性质划分	新建项目、扩建项目、改建项目、迁建项目、恢复项目
按照复杂程度划分	复杂项目、简单项目
按照项目结果划分	产品项目、服务项目
按照行业领域划分	农业项目、工业项目、投资项目、建设项目、教育项目、社会项目
按照用户状况类别划分	明确用户的项目、无明确用户的项目
按照投资使用方向和投资主体的活动范围划分	竞争性项目、基础性项目、公益性项目

2.3.2 项目管理概述

项目管理是伴随着技术进步和项目的复杂化、大型化而逐渐形成的一门管理学科，它以项目为研究对象，在有限的资源限定条件下，通过临时性的开发组织对项目进行高效率的计划、组织、实施和监管，动态管理项目过程，最终实现或超过设定的需求和期望的过程。

“项目”这一概念很早就诞生了，它可以追溯到数千年之前，例如古埃及的金字塔、中国的万里长城和都江堰、印度的泰姬陵、巴比伦的空中花园等，这些著名工程体现了项目管理的概念和技术。只要有项目的建设就会有相应的项目管理问题。例如，我国北宋真宗年间，皇宫失火，将皇宫烧成废墟，宋真宗命令丁渭主持修改皇宫的工程，此工程时间紧迫，工程规模庞大，而且皇宫结构比较复杂。那么如何在有限的时间和资源条件下，以最小的代价、最快的速度完成这项工程便成为一大难题。在对废墟的勘察中丁渭发现了三个难题：第一是取土困难；第二是运输困难；第三是清理废墟困难。在明确主要问题后，制定了详细的解决方案：沿皇宫前门大道至汴水河岸挖道取土，将大道挖成小河道，挖出的土用来烧瓦，解决“取土困难”。挖成河道接通汴水，建筑材料可由小河道直运工地，解决了“运输困难”。皇宫修复后，将建筑垃圾填到小河道内，恢复原来的大道，解决了“清理废墟困难”。这个项目运用“大道变河道”“挖土来烧瓦”“废墟填河道”这三个事件的相互关系，使整个工程系统有序进行并向理想的方向发展，这也许是古人成功地进行项目管理的先例。虽然项目管理的思想在古代就有体现，但是直到 21 世纪初，一套科学的项目管理理论和项目管理技术依然没有形成体系，绝大多数的项目依然依靠个人的经验和直觉，项目在管理上根本不具有科学性。

在上述案例中，项目管理方法在实践中取得成功的例子使得人们越来越重视项目管理的理论和方法，它对提高项目的管理效率起到了重要作用。

近代项目管理始于 20 世纪 30 年代，最初由亨利·L. 甘特发明的甘特图进行项目的规划和控制，这种图直观地反映了项目的过程管理与进度，但是对于规模较大、内容复杂的项目而言，甘特图就不能综合地反映项目本身的完成情况。直到 1931 年，由卡罗尔·阿丹密

基研制的协调图克服了这一缺点，但是这项研究并没有得到人们的重视。早期，人们虽然运用项目管理的方法和技术，但是对于项目管理的概念没有清晰的理解，项目管理的概念也缺乏科学的理论指导。第二次世界大战后，项目管理的概念被提出与曼哈顿的计划有关。进入20世纪50年代，杜邦公司在一个价值千万美元的化工项目运用了关键路径法，大大缩短了工期，节约了10%的投资；美国海军研究北极星式导弹的应急项目通过运用计划评审技术开发出来，该项目解决了200多个承包商的组织协调问题。发展到60年代，网络技术被应用到美国的特大型项目阿波罗载人登月计划，采用这一技术，使整个项目的运筹和组织工作进行得有条不紊。到现在，项目管理已经与人们的日常生活息息相关，不可分割。

了解了项目管理的发展过程，那么项目管理究竟是什么？与项目的概念相对应，项目管理是在一定的时间期限和有限的资源约束下，为了完成一个既定的目标，通过项目经理和项目组织的合作，有效地计划、组织、领导和控制项目，使项目达到既定目标。项目管理是综合应用理论和经验知识，在各种资源约束下寻找实现预定目标最佳的组织安排和管理方法。所以，项目管理是理论知识与经验的有机结合，两者缺一不可，一个优秀的项目经理应该是具有扎实的理论功底，经过多个项目管理磨炼出来的管理者。

项目管理具有以下基本特点。

(1) 项目管理是一项复杂的工作。

项目的建设时间跨度长、涉及面广、过程复杂。项目管理需要各方面的人员相互协调，要求全体人员能够综合运用包括专业技术、经济、法律等多种学科知识，步调一致地进行工作，随时解决工程项目建设过程中发生的问题。

(2) 项目管理具有创造性。

项目具有一次性的特点。没有两个完全相同的项目。项目管理者必须从实际出发，结合项目的具体情况，因地制宜地处理和解决项目实际问题。因此，项目管理就是将前人总结的知识和经验，创造性地运用于项目管理实践。

(3) 项目管理需要集权领导和建立专门的项目组织。

项目管理需要对资金、人员、材料、设备等多种资源、进行优化配置和合理使用，需要专门机构、专业人才进行专业化管理。

(4) 项目管理者或项目经理在项目管理中起着非常重要的作用。

项目经理是项目管理的核心，一个好的项目背后必然有一个优秀的项目经理。项目经理必须能够了解、利用和管理项目的技术方面的复杂性，必须能够综合各种不同的专业观点来考虑问题。但仅具备技术知识和专业知识仍是不够的，成功的管理还取决于预测和控制人的行为的能力。项目经理的最终职责是确保工作在预算内按时优质地完成，使客户满意。激励项目团队，赢得顾客的信任，是项目经理必备的技能。

2.3.3 项目管理的过程

项目管理是由一系列的项目阶段或工作过程构成的，任何项目都可以划分为多个不同的项目阶段或项目工作过程，这些过程相互交叉，相互作用。美国项目管理协会把项目管理分成5个过程组：启动、计划、执行、控制和结束，这些过程组贯穿于项目的整个生命周期。

只有完成了本过程工作，才能进入下一个过程，不可盲目逾越。

1. 启动过程

启动过程就是一个新项目的识别和开始的过程，它定义了某一个项目阶段的工作开始与否，如果项目不能满足用户需求，那么项目就会终止。

启动过程所包含的管理内容有：定义一个项目或项目阶段的工作与活动，决策一个项目或项目阶段的启动与否，或决策是否将一个项目或项目阶段继续进行下去等工作，这是由一系列项目决策性工作所构成的项目管理具体过程。

2. 计划过程

计划过程也称为规划过程，它是项目管理过程中最复杂也是最重要的一个阶段。因为这个阶段涉及了项目范围管理、时间管理、成本管理、质量管理、沟通管理、人力资源管理、风险管理、采购管理、集成管理等9个方面，它贯穿于项目管理的整个生命周期。如果项目发生重大变化，就必须对以往的计划进行重新审查。

计划过程所包含的管理内容有：拟订、编制和修订一个项目或项目阶段的工作目标、工作计划方案、资源供应计划、成本预算、计划应急措施等方面的工作。

3. 执行过程

项目执行阶段，也叫项目实施阶段，需要完成项目管理计划中确定的工作，这样才能满足项目规范要求。

执行过程包含的管理内容有：组织和协调人力资源和其他资源，组织和协调各项任务与工作，激励项目团队完成既定的工作计划，生成项目产出物等方面的工作。

4. 控制过程

项目控制阶段也是一个非常重要的阶段，它在整个项目过程中发挥着监督作用，能够保证项目顺利、正确地实施。

控制过程包括的管理内容有：制定标准、监督和测量项目工作的实际情况、分析差异和问题、采取纠偏措施等管理工作和活动。这些都是保障项目目标得以实现，防止偏差积累而造成项目失败的管理工作与活动。

5. 结束过程

进入项目收尾阶段，意味着项目管理过程中的各个阶段都已经完结，整个项目正式结束。

结束过程包括的管理内容有：制定一个项目或项目阶段的移交与接收条件，项目或项目阶段成果的移交，从而使项目顺利结束的管理工作和活动。

项目管理的过程不是独立的一次性事件，它们是贯穿项目每一个阶段强度有所变化的互相重叠的活动。图2-2说明了一个项目阶段的各个过程是如何重叠和变化的。

项目管理的过程还与它们产生的结果联系起来。一个过程的结果将成为另一个过程的依据。一个项目阶段内各过程的相互关系如图2-3所示。

在项目每一个阶段都包括上述基本过程，一个过程在上一个阶段的结束为下一个阶段的发起提供依据。

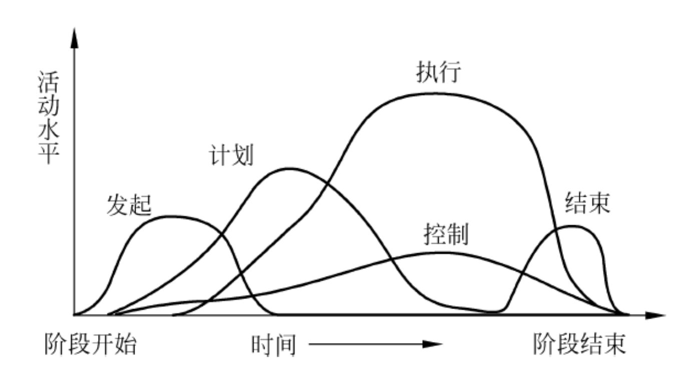


图 2-2　一个项目阶段各过程的重叠

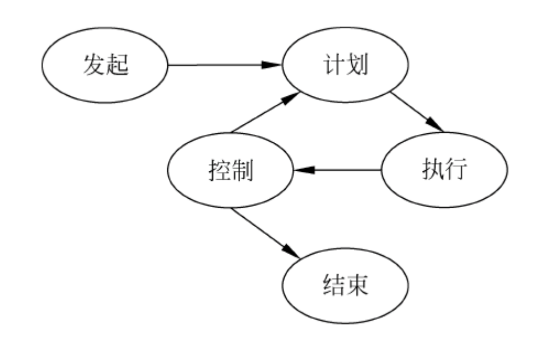


图 2-3　一个项目阶段内各过程的相互关系

2.3.4　项目管理的要素

项目管理有四个要素：范围(Scope)、时间(Time)、成本(Cost)、质量(Quality)。对于一个项目来说最理想的情况就是“多、快、好、省”。“多”指工作范围大，“快”指时间短，“好”指质量高，“省”指成本低。但是，这 4 者之间是相互关联的，提高一个指标的同时会降低另一个指标，所以实际上这种理想的情况很难达到。项目管理的四大要素如图 2-4 所示。

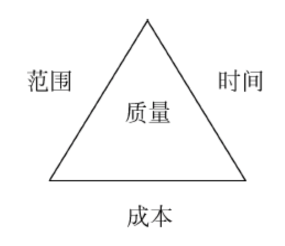


图 2-4　项目管理的四大要素

1. 范围

范围也称工作范围，指为了实现项目目标必须完成的所有工作。一般通过定义交付物和交付物标准来定义工作范围。工作范围根据项目目标分解得到，它指出了“完成哪些工作可以达到项目的目标”，或者说“完成哪些工作项目就可以结束了”。后一点非常重要，如果没有工作范围的定义，项目就可能永远做不完。要严格控制工作范围的变化，一旦失控就会出现“出力不讨好”的尴尬局面：一方面做了许多与实现目标无关的额外工作；另一方面却因额外工作影响了原定目标的实现，造成商业和声誉的双重损失。

2. 时间

与项目时间相关的因素用进度计划描述，进度计划不仅说明了完成项目工作范围内所有工作需要的时间，也规定了每个活动的具体开始和完成日期。项目中的活动根据工作范围确定，在确定活动的开始和结束时间还要考虑它们之间的依赖关系。

3. 成本

成本指完成项目需要的所有款项，包括人力成本、原材料、设备租金、分包费用和咨询费用等。项目的总成本以预算为基础，项目结束时的最终成本应控制在预算内。特别应注意的是，在IT项目中人力成本比例很大，而工作量又难以估计，因而制定预算难度很大。

4. 质量

质量指项目满足明确或隐含需求的程度。一般通过定义工作范围中的交付物标准来明确定义这些标准，包括各种特性及这些特性需要满足的要求，因此交付物在项目管理中有重要的地位。另外，有时还可能对项目的过程有明确要求，如规定过程应该遵循的规范和标准，并要求提供这些过程得以有效执行的证据。

时间、质量、成本这三个要素简称TQC(Time Quality Cost)。在实际工作中，工作范围在合同中定义，时间通过进度计划规定，成本通过预算规定，而如何确保质量在质量保证计划中规定。这几份文件是一个项目立项的基本条件。一个项目的工作范围和TQC确定了，项目的目标也就确定了。如果项目在TQC的约束内完成了工作范围内的工作，就可以说项目成功了。

综上所述，项目的成功就是指“客户满意、公司获利”，这取决于多种因素，包括项目前真正了解什么是客户的成功，明确成功的标准；项目中定义清晰工作范围和TQC，并按TQC的约束完成工作范围；项目后帮助客户实现商业价值。只有当客户说项目成功时，才是项目的真正成功。

2.4 小　　结

把信息安全作为一个整体的工程来进行研究，是系统工程理论和方法影响作用的结果。其中，系统工程思想、项目管理方法、质量管理体系都是支撑信息安全工程的理论基础，掌握这些理论基础，可以更好地理解信息安全工程思想。

习　　题

1. 简述系统的定义和一般特征。
2. 为什么说系统工程是一门交叉的新兴学科？
3. 质量管理经历了哪些发展阶段？各阶段有何特点？
4. 如何开展一个IT项目的项目管理？

第3章　信息系统安全工程

本章学习目标：

- 了解信息系统安全工程基本概念。
- 了解信息系统安全工程过程。
- 掌握如何基于信息系统安全工程方法开展系统安全工程建设。

3.1　概　　述

信息安全保障问题的解决既不能只依靠纯粹的技术，也不能只靠简单的安全产品的堆砌，它要依赖于复杂的系统工程，即信息安全工程。本章主要介绍由系统工程发展而来，以时间维划定工程元素的方法学——信息系统安全工程。

3.1.1　信息系统安全工程的定义

1993年，美国国家安全局制定的《信息系统安全工程手册》中提出了“信息系统安全工程”(Information Systems Security Engineering，ISSE)的概念，并将其定义为“侧重于信息安全的应用系统工程”。美国国家安全局2000年制定的《国家信息系统安全术语表》(NSTISSI No.4009)中，将ISSE描述为“在信息系统生命周期过程中为实现和维护系统最优的安全性和持续性所做的各种努力”。现在对ISSE的普遍解释为：“信息系统安全工程是采用工程的概念、原理、技术和方法，来研究、开发、实施与维护信息系统安全的过程，是将经过时间考验证明是正确的工程实践流程、管理技术和当前能够得到的最好的技术方法相结合的过程”。

信息系统安全工程是系统工程在安全空间的映射，它的重点是通过实施系统工程过程来满足信息保护的需求，信息系统安全工程将有助于开发可满足用户信息保护需求的系统产品和过程解决方案，信息系统安全工程的主要目标包括以下6个方面。

(1) 获得对企业安全风险的理解。

(2) 根据已识别的安全风险建立一组平衡的安全需求。

(3) 将安全需求转换成安全的策略，成为信息系统建设基本原则，并落实到项目实施中的各个科目活动、系统配置或运行的定义中。

(4) 通过正确有效的安全机制建立抵御安全威胁和系统正常运营的保证。

(5) 动态监测和判断系统中和系统运行时出现的安全隐患和突发事件，并及时按预先指定的方案，启动紧急事故处理程序进行处理和追踪，遏制危险的发生和蔓延，使系统免除

损失或控制在可控制范围之内。

(6) 将所有科目和专业活动集成为一个具有共识的系统安全可信性工程。

3.1.2 信息系统安全工程与系统工程的关系

系统工程是信息系统安全工程的基础，通常系统工程可以分为发掘需求、定义系统、设计系统和实施系统4个阶段，在这4个阶段的执行过程中还需要有阶段性评估。信息系统安全工程是系统工程的一部分，是系统工程的基本原理在信息安全领域内的具体应用，它也分为发掘信息保护需求、定义信息保护系统、设计信息保护系统和实施信息保护系统4个阶段，每个阶段还可以进一步细分，在这4个阶段的执行过程中同样还必须有阶段性评估，以保证执行效果。

具体来说，一个信息系统安全工程包括发掘信息保护需求、定义信息保护系统、设计信息保护系统、实施信息保护需求以及评估信息保护系统几个步骤。信息系统安全工程(ISSE)与系统工程(SE)的对应关系如图3-1所示。

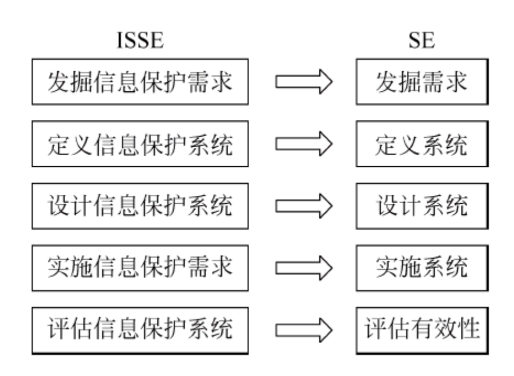


图3-1 信息系统安全工程与系统工程的对应关系

对系统而言，ISSE过程和SE过程要同步考虑：即在相应的阶段同时考虑信息保护的目标、需求、功能、体系结构、设计、测试与实施，使得信息保护得以优化。它们的具体区别如表3-1所示。

表3-1 SE过程与ISSE过程的区别

SE过程	ISSE过程
发掘需求	发掘信息保护需求
系统工程师要帮助客户理解并记录用来支持其业务或使命的信息管理的需求，信息需求说明可以在信息管理模型(Information Management Model，IMM)中记录	信息系统安全工程师要帮助客户理解用来支持其业务或使命的信息保护的需求。信息保护需求说明可以在信息保护策略(Information Protection Policy，IPP)中记录
定义系统	定义信息保护系统
系统工程师要向系统中分配已经确定的需求。应标识出系统的环境，并说明系统功能对该环境的分配。要写出概要性的系统运行概念(Concept of Operations，CONOPS)，描述待建系统的运行情况。要建立起系统的基线要求	信息系统安全工程师要将信息保护需求分配到系统中。系统安全的背景环境、概要性的系统安全CONOPS以及基线安全要求均应得到确定

续表

SE 过程	ISSE 过程
设计系统	设计信息保护系统
(1) 设计系统体系结构 系统工程师应该分析待建系统的体系结构，完成功能的分析和分配，同时分配系统的要求，并选择相关机制。系统工程师还应确定系统中的组件或要素，将功能分配给这些要素，并描述这些要素间的关系。 (2) 开展详细设计 系统工程师应分析系统的设计约束和均衡取舍，完成详细的系统设计，并考虑生命周期的支持。系统工程师应将所有的系统要求跟踪至系统组件，直至无一遗漏。最终的详细设计结果应反映出组件和接口规范，为系统实现时的采办工作提供充分的信息	(1) 设计系统安全体系结构 信息系统安全工程师要与系统工程师合作，一起分析待建系统的体系结构，完成功能的分析和分配，同时分配安全服务，并选择安全机制。信息系统安全工程师还应确定安全系统的组件或要素，将安全功能分配给这些要素，并描述这些要素间的关系。 (2) 开展详细的安全设计 信息系统安全工程师应分析设计约束和均衡取舍，完成详细的系统和安全设计，并考虑生命周期的支持。信息系统安全工程师应将所有的系统安全要求跟踪至系统组件，直至无一遗漏。最终的详细安全设计结果应反映出组件和接口规范，为系统实现时的采办工作提供充分的信息
实施系统	实施信息保护需求
系统工程师将系统从规范变为现实，该阶段的主要活动包括采办、集成、配置、测试、记录和培训。系统的各组件要接受测试和评估，以确保它们能够满足规范。成功的测试之后，各组件——硬件、软件、固件要进行集成和正确的配置，并作为一个系统接受整体测试	信息系统安全工程师要参与到对所有的系统问题进行的多学科检查之中，并向 C&A 过程活动提供输入，例如检验系统是否已经针对先前的威胁评估结果实施了保护；跟踪系统实现和测试活动中的信息保护保障机制；向系统的生命周期支持计划、运行流程以及维护培训材料提供输入
评估有效性	评估信息保护系统
各项活动的结果要接受评估，以确保系统能够满足用户的需求，系统在一个预期环境中实现了期望的功能，并达到了一个需要的质量标准。系统工程师要检查系统对任务需求的满足程度	信息系统安全工程师要关注信息保护的有效性——系统是否能够为其使命所需的信息提供保密性、完整性、可用性、认证和不可否认性

3.2　信息系统安全工程过程

3.2.1　发掘信息保护需求

ISSE 的过程始于审视用户的任务需求、相关政策、规定、标准以及用户环境中的信息系统威胁。ISSE 随后要确定信息系统和信息的用户是谁、与其他信息系统和信息进行交互的状态如何，以及在信息保障系统生命周期的每个阶段，它们的角色、职责和授权是什么。信息保障需求应当来自用户的观点，而不应过度受限于信息设计或实施的限制。

发掘信息保护需求要考虑以下方面。

(1) 考虑对所要完成任务的信息保护需求。

(2) 掌握对信息系统的威胁。

（3）考虑信息保障政策。

发掘信息保障需求过程和主体如图 3-2 所示。

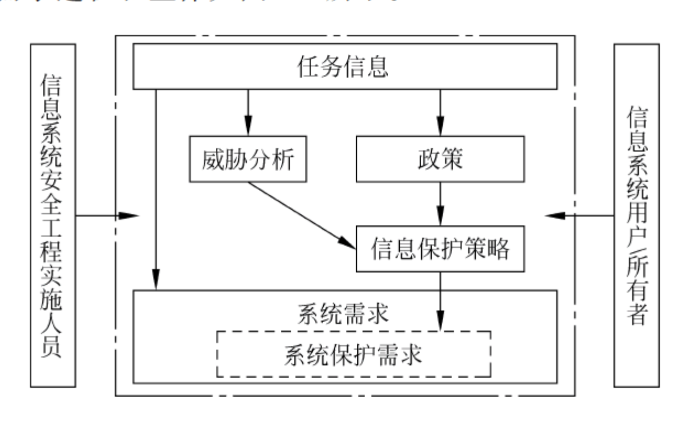


图 3-2　发掘信息保障需求过程和主体

1. 考虑对所要完成任务的信息保护需求

ISSE 首先需要考虑系统任务可能受到的各方面的影响（包括人的因素和系统的因素），以及可能造成的各方面的损失，例如泄密、数据被篡改、服务不可用、操作抵赖等。用户通常都知晓其所需要的任务信息的重要性，但在确定这些信息需要何种保护，以及达到怎样的保护级别时，可能会一筹莫展。为了科学地了解任务的信息保护需求，ISSE 需要做的工作如下。

（1）帮助用户对信息处理的过程建模。

（2）帮助用户定义对信息的各种威胁。

（3）帮助用户确定信息的保护次序和等级。

（4）制定信息保护策略。

（5）与用户协调、达成一致。

与用户进行交互是 ISSE 的必不可少的环节，在标识信息系统和信息的具体用户，标识用户与信息系统和信息的交互作用的实质、用户在信息保护生命周期各阶段的角色、责任和权力的基础上，评估信息和系统对任务的重要性，并确保任务需求中包含了信息保护的需求、系统功能中包含了信息保护的功能。

这个环节要达到的目标是：一份满足用户在资金、安全、性能、时间等各方面要求的信息系统保护框架，其中至少要包含以下几个方面。

（1）被处理的信息是什么？属于何种类型（涉密信息、金融信息、个人隐私信息等）？

（2）谁有权处理（初始化、查看、修改、删除等）这些信息？

（3）授权用户如何履行其职责？

（4）授权用户使用何种工具（硬件、软件、固件、文档等）进行处理？

（5）用户行为是否需要监督（不可否认）？

在这个环节，ISSE 的工作需要用户的全程参与，共同研究信息系统的角色，使信息系统更好地满足用户的任务要求。

2. 掌握对信息系统的威胁

定义信息面临的威胁是“发掘信息保护需求”的一项关键活动。“威胁”是指可能造成某

个结果的事件或对系统造成危害的潜在事实。对信息管理的威胁，是指可以利用信息系统的脆弱性，可能造成某个有害结果的事件或对信息系统造成危害的潜在事实。

ISSE 需要在用户的帮助下，准确、详尽地定义出信息系统在设计、生产、使用、维护以及销毁的过程中可能受到的威胁，并针对这些威胁提出相应策略。

分析信息系统面临的安全威胁，可以从以下几个方面入手。

(1) 检测恶意攻击。指检测人为的、有目的性的破坏行为，这些破坏行为分为主动和被动两种。主动攻击是指以各种方式有选择性地破坏信息，例如欺骗、修改、删除、否决、伪造、信息泄露、拒绝服务、提升权限等；被动攻击是指在不干扰系统正常工作的情况下，进行侦听、截获、窃取、破译等。

(2) 了解安全缺陷。指了解信息系统本身存在的一些安全缺陷，包括网络硬件、通信链路、人员素质、安全标准等原因引起的安全缺陷。

(3) 掌握软件漏洞。因为软件的复杂性和编程方法的多样性，导致软件中有意或无意留下了一些漏洞，例如操作系统的安全漏洞、TCP/IP 协议的漏洞、网络服务的漏洞等。

(4) 分析结构隐患。主要是指网络拓扑结构的安全隐患，因为诸如总线、星状、环状、树状等结构都有各自的优缺点，都存在相应的安全隐患。

分析信息的威胁主体，应该涉及以下几个方面。

(1) 威胁主体的动机或意图。

(2) 威胁主体的能力。

(3) 威胁或攻击的途径。

(4) 主体及威胁存在的可能性。

(5) 影响或后果。

3. 考虑信息保障政策

在了解了信息保护需求并掌握了系统面临的威胁之后，ISSE 需要考虑信息保障政策，并制定出相关的信息安全策略。

策略是指以正式形式出现的，经管理层同意和批准的，规定了组织行为方向和行为自由程度的途径，或者说策略是管理层对某个主题有关意见的一种陈述形式。信息安全策略是一组规则，这组规则描述了一个组织要实现的信息安全目标和实现这些信息安全目标的途径。

从管理角度看，信息安全策略是一个组织关于信息安全的文件，是一个组织关于信息安全的基本指导规则。它通常由组织最高管理层批准，在整个组织内发布。其目标在于减少信息安全事故的发生，将信息安全事故的影响与损失降低到最小。信息安全策略必须由高层管理机构批准并颁布，在策略的贯彻过程中，应该使每个参与者都能够理解策略，并且理解为相同的含义。如果策略在某些地方不能得到贯彻，则一定要让其他参与者都知道这样做的后果。信息安全策略是分层的，一旦制定后，高层的策略一般是不会改变的，而下层的局部策略可以根据具体情况而定，但不能与更高层的信息安全策略及其他有关政策相违背。制定策略的时候需要全面考虑相关的国家政策、法规、标准和惯例等。为达成这个目标，策略制定小组不仅需要系统工程师、ISSE 工程师、用户代表，还需要信用机构、认证机构、设计专家，甚至是政府机构的参与。

信息安全策略中需要具体定义出要保护什么、用什么方法保护、如何保护，需要确定以

下几方面的内容。

(1) 法律和法规。所要遵循的相关法律和法规的要求。

(2) 信息保护的内容和目标。确定要保护的所有信息资源,以及它们的重要性、所面临的主要威胁和需要达到的保护等级。

(3) 信息保护的职责落实办法。明确各组织、机构或部门的信息安全保护的责任和义务。

(4) 实施信息保护的方法。确定保护信息系统中的各种信息资源的具体方法。

(5) 事故的处理。包括应急响应、数据恢复等措施,以及相应的奖惩条款、监督机制等。

3.2.2 定义信息保护系统

ISSE将定义信息保护系统将要做什么、信息保护系统执行其功能的情况如何,以及信息保护系统的内部和外部接口。定义信息保护系统的活动时,用户对于信息保障需求和信息系统环境的描述要被转换成目标、要求和功能,这一工作是要定义需要建立什么样的信息保障系统、信息保障系统如何实现良性地运行,并定义信息保障系统的内/外部接口,包括以下内容。

(1) 确定信息保障目标。

(2) 描述系统内部关联和环境。

(3) 检查信息保障要求。

(4) 功能分析。

1. 确定信息保障目标

信息保障目标与通常的系统对象具有相同的特性,例如对于信息保护需求的明确性、可测量性、可验证性、可追踪性等。确定信息保护对象,要保证它们的这些有效性度量(Measure of Effectiveness,MoE)性质,在描述每个对象时需要说明以下问题。

(1) 信息保障目标支持系统中的什么任务对象。

(2) 有哪些与信息保护目标和任务相关的威胁。

(3) 失去目标会有什么后果。

(4) 受什么样的信息保护策略或方针的支持。

2. 描述系统内部关联和环境

在信息安全工程中,系统联系对于确定系统边界并实施保护是很重要的,任务目标、任务信息处理、系统威胁、信息安全策略、设备等都极大地影响着系统边界与环境,因此,描述系统内部关联和环境需要做以下工作。

(1) 在系统的任务处理过程、与其他系统和环境之间,确定物理的和逻辑的边界。

(2) 描述信息的输入和输出、系统与环境之间或与其他系统之间的信号与能量的双向流动情况。

3. 检查信息保障要求

ISSE的系统信息保障要求检查任务是对上述过程中的分析(包括目标、任务、威胁、系统联系等)进行特征检查。当信息保护需求从最初的信息保障的用户愿望,经过充分定义,并演变为一系列的系统保护规范时,信息保护的需求能力可能出现缺失,因此,需要检查信

息保护需求的正确性、完整性、一致性、依赖性、无冲突和可测试性等特征。

4. 功能分析

ISSE 使用许多系统工程工具来理解信息保护功能，并将功能分配给系统中各种信息保护的配置项。在定义信息保护系统中，对功能进行分析，必须分析备选系统体系结构、信息保护配置项，以及信息保护子系统是如何成为整个系统的一部分，这些功能是否能达到原本设定的目标，并理解它们如何才能与整个系统协调工作。

3.2.3　设计信息保护系统

明确目标系统后，将构造信息系统的体系结构，详细说明信息保护系统的设计方案。这时 ISSE 工程师要进行如下工作。

(1) 功能分配。

(2) 信息保护预设计。

(3) 详细信息保护设计。

1. 功能分配

当某种系统功能被定位到人、软件、硬件或固件上后，同时也就附上了相对应的信息保护功能。ISSE 应该为系统制定一个理论和实践上都可行的、协调一致的信息保护系统体系构架。功能分配过程包括以下内容。

(1) 提炼、验证并检查安全要求与威胁评估的技术原理。

(2) 确保一系列的低层要求能够满足系统级的要求。

(3) 完成系统级体系结构、配置项和接口定义。

2. 信息保护预设计

在需求和构架已经确定的前提下，ISSE 进入了信息保护的预设计阶段。在这一阶段，ISSE 工程师将制定出系统建造的规范，其中至少包括以下内容。

(1) 检查、细化并改进前期需求和定义的成果，特别是配置项的定义和接口规范。

(2) 从现有解决方案中找到与配置项一致的方案，并验证是否满足高层信息保护要求。

(3) 加入系统工程过程，并支持认证/认可和管理决策，提出风险分析结果。

3. 详细信息保护设计

进一步完善配置及方案，细化底层产品规范，检查每个细节规范的完整性、兼容性、可验证性、安全风险和可追踪性等。详细设计包括以下内容。

(1) 检查、细化并改进预设计阶段的成果。

(2) 对解决方案提供细节设计资料，以支持系统层和配置层的设计。

(3) 检查关键设计的原理和合理性。

(4) 设计信息保护测试与评估程序。

(5) 实施并追踪信息保护的保障机制。

(6) 检验配置层设计与上层方案的一致性。

(7) 提供各种测试数据。

(8) 检查和更新信息保护的风险与威胁计划。

(9) 加入系统工程过程，并支持认证/认可和管理决策，提出风险分析结果。

3.2.4 实施信息保护需求

这一活动的目标是建立、采购、集成、核实和验证各个信息保障的子系统，包括按照计划更新对于系统信息保障威胁的评估，以及对于系统运作状况的评估；核实系统信息保障要求以及实施解决方案的限制；跟踪、参与和应用信息保障担保机制；考查系统运行过程的进展情况，包括生命周期的支持计划；一套正式的信息保障评估系统；对于验证和鉴定过程的活动进一步增加内容；参与集体的、多学科的综合检查。

具体内容包括以下三个阶段。

(1) 采购部件。

(2) 建设系统。

(3) 测试系统。

1. 采购部件

一般来说，要根据市场产品的研究、偏好和最终的效果，来决定是以购买还是自行生产的方式来取得部件。购买/生产的决定应该通盘考虑安全因素、可操作性、性能、成本、进度、风险等影响。在购买时，对于大量生产且相对低成本的商业现货供应(Commercial off the Shelf，COTS)和由政府机构创建的技术团体开发的政府现货供应(Government off the Shelf，GOTS)等都可作为部件采购的考虑范围。在采购部件时，要注意考虑以下因素。

(1) 确保考虑了全部相关的安全因素。

(2) 查看现有产品是否能满足系统部件的需求，最好有多种产品可供选择。

(3) 验证一系列潜在的可行性选项。

(4) 考虑将来技术的发展，新技术和新产品如何运用到系统中去。

2. 建设系统

建设系统的过程，是确保已设计出必要的保护机制，并使该机制在系统实施中得以实现。与许多系统一样，信息保护系统也会受到许多因素的影响来加强或削弱其效果，这些因素决定了信息保护对系统的适宜程度。所以，在建设系统中，要重视以下问题。

(1) 部件的集成是否满足系统安全规范。

(2) 部件的配置是否保证了必要的安全特性，以及安全参数能否正确配置以便提供所要求的安全服务。

(3) 对设备、部件是否有物理安全保护措施。

(4) 组装、建造系统的人员是否对工作流程有足够的知识和权限。

3. 测试系统

ISSE要给出一些与信息保护相关的测试计划和工作流程，还要给出相关的测试实例、工具、软硬件等。这些测试系统的工作包括以下内容。

(1) 检查、细化并改进设计信息安全系统的阶段结果。

(2) 检验解决方案的信息保护需求和约束限制等条件，并实施相关的系统验证和确认机制与决策。

(3) 跟踪实施与系统实施和测试相关的系统保障机制。

(4) 鉴别测试数据的可用性。

(5) 提供安全支持计划,包括逻辑上的、有关维护和培训等方面。

(6) 加入系统工程过程,并支持认证/认可和管理决策,提出风险分析结果。

3.2.5　评估信息保护有效性

ISSE集中于信息保障系统的有效性,主要是指系统在保密性、完整性、可用性、不可否认性等安全特性方面的有效性。如果系统在这些方面达不到要求,信息系统安全工程的任务则很难达到用户的满意。

有效性评估要注意以下几点。

(1) 系统的互操作安全性,即系统是否通过外部接口正确地保护了信息。

(2) 系统的可用性,即系统是否能给用户提供信息资源与信息保护。

(3) 用户需要接受什么样的培训才能正确地操作和维护信息保护系统。

(4) 人机界面或接口是否有缺陷,从而导致出错。

(5) 建造和维护信息系统的成本是否可以接受。

(6) 确定风险和可能的任务影响,并提供报告。

要在多项活动中评估信息保护的有效性:发掘信息保护需求,定义系统安全要求,定义系统安全体系结构,开展详细的安全设计以及实现系统安全。

3.3　基于ISSE的公文流转系统安全解决方案

公文流转系统就是利用网络传送工作文件,将工作流转化为电子信息流,实现发文、收文、签发、审批等行政事务信息化,它的目的在于推进各部门办公自动化、网络化、电子化,通过信息及通信技术的应用,改变目前各部门之间传统的手工公文流转方式,突破时间与地域限制,使成员之间真正通过电子化渠道进行沟通,提高工作效率,从而为进一步实现信息化打下良好基础。

3.3.1　公文流转系统概述

公文管理是各企事业单位最繁杂的一项工作,不仅工作量非常大而且公文种类也很多。它主要包括议案、请示、工作报告、通报、通知、公告、函件、工作总结等。收文管理和发文管理是公文流转系统的核心功能,此安全解决方案主要针对收文管理和发文管理过程中的安全问题展开。

收文管理包括收文登记、收文拟办、核签、审核、批示、批复意见填报、收文办理、归档等工作。收文登记时自动编制收文号,可以选择模板或以附件形式新建公文。根据收文流程自动进行公文流转。收文办理人可以查看正文和历史处理流程、意见,收文流程如图3-3所示。

发文管理完成发文工作中的全部业务工作。在发文管理中文件由起草部门进行正式的拟稿,然后通过工作流送交部门负责人复核,在核稿完成后,送交主管领导审批并提交主管领导签发,完毕后返回经办人,由经办人清稿后发给办公室进行分发传阅,全部阅示完毕后文件归档。发文流程如图3-4所示。

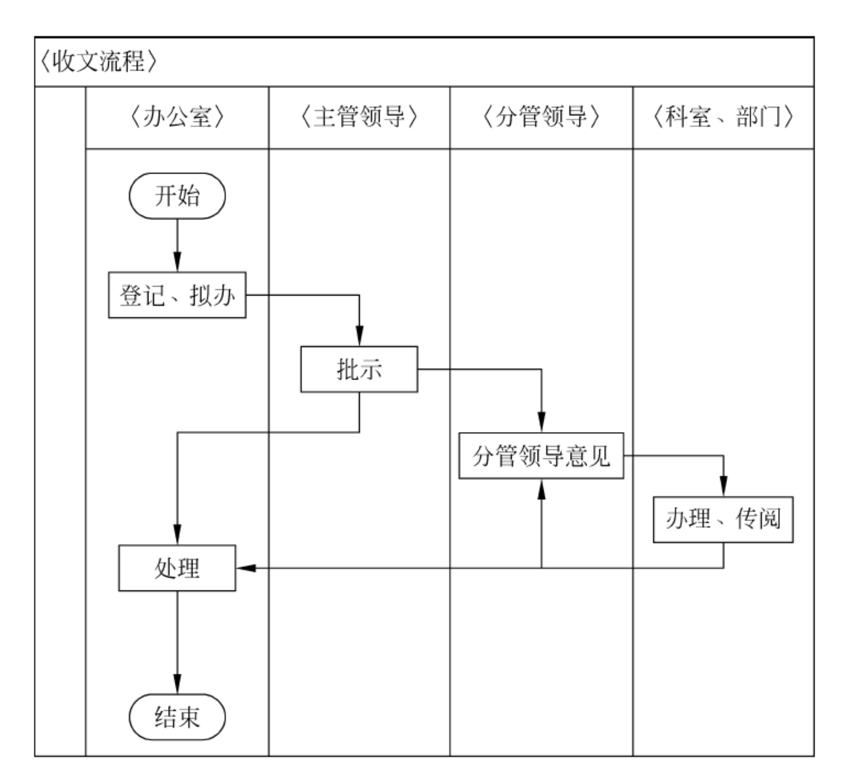


图 3-3 收文流程

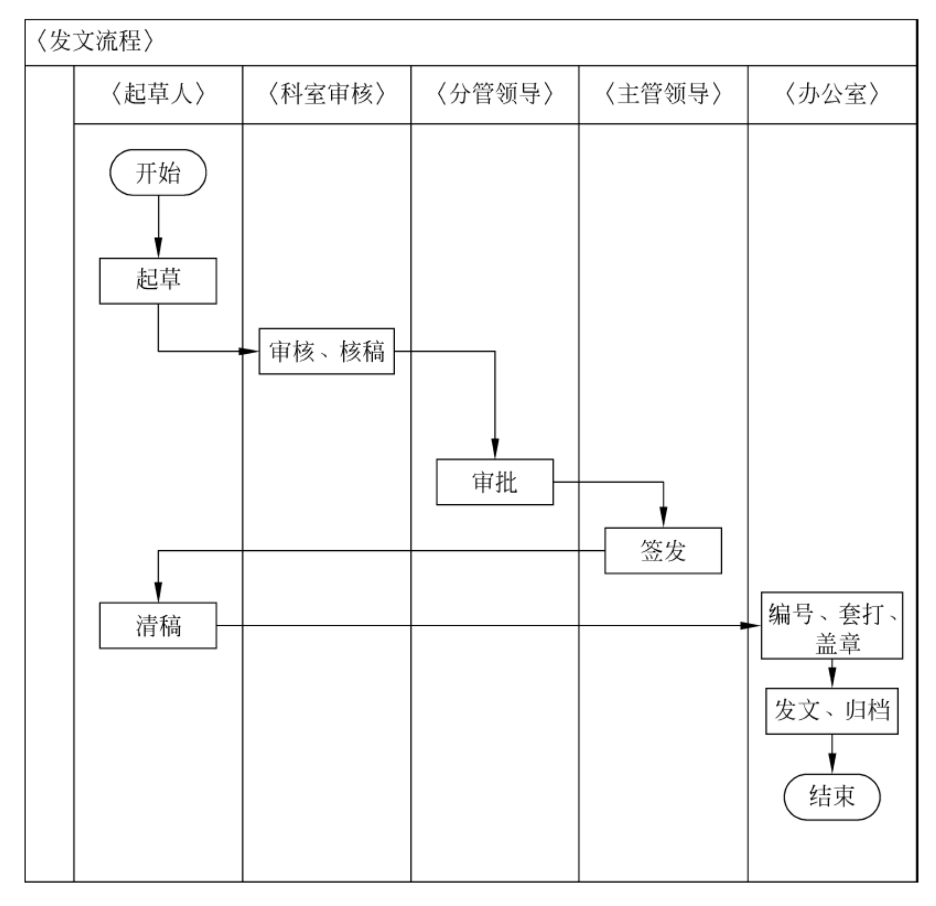


图 3-4 发文流程

从发文管理与收文管理的具体流程不难发现，公文流转强调一级一级处理的流程，不能越级也不能回转，因此访问控制是流程正常运行的关键；公文流转需要参与角色具有相应的权限才能进行既定的操作，由此可见身份认证也是一个必不可少的环节，此外，公文传输过程中的安全问题，也是一个不容忽视的环节。

3.3.2　安全需求分析

1. 公文流转系统的特点

公文流转系统包括了公文的上传、审批、下达、查阅等环节，是一种特殊的管理信息系统。公文流转系统能根据用户提出的公文流程，对整个工作流程进行实时跟踪，对修改审核的信息进行记录，并能根据有关规定自动地报告公文在流转过程中的状态。其特点主要体现在以下几个方面。

（1）公文流转系统处理的是公文，涉及的往往是一些非结构化数据，没有结构、类型等方面的规定，不同的公文有不同的处理流程。

（2）公文流转系统是集中式与分布式的混搭。公文集中存储在服务器上，在应用程序驱动下，在公文处理的各个环节流转。关于公文处理终端功能，有些需要能支持在本地进行扫描、编辑等公文处理，应用分布式，有些只需要支持批阅公文，需要集中式。

（3）公文流转系统中公文的安全级别不同。公文流转系统应用于许多的办公部门，每个部门的工作人员的权限应该是不同的。公文流转过程中针对不同层次、级别的办公人员而言，公文的保密程度不同。

（4）公文流转系统是一种综合性的管理系统，人员之间的协同工作在系统处理过程中表现尤为重要，公文流转过程中每个经手的人员或者部门的权限应该不同。用户可以预先定义公文的处理流程及相应权限，只有具有相应权限的人员才可以进行公文的在线处理。

2. 确定威胁类别及所带来的影响

威胁分析是安全需求挖掘中有决定意义的一步，只有确定威胁的种类，才能针对特定的威胁种类定义出特定的安全策略，制定有效的安全方法。对于整个公文流转系统，所受的威胁主要来自于以下两个方面。

1）使用网络访问的人

（1）来自系统内部人员的威胁。一方面，可能由于员工对于系统的安全操作要求不达标，从而导致系统运行无法达到安全标准，还有用户的不安全的使用习惯导致的系统的不安全；另一方面，可能由于员工有意恶意操作导致系统的不安全。

（2）来自系统外部人员的威胁。由于系统内部的有些公文具有一定的价值，导致系统外部人员对系统发起攻击，从而对系统安全造成威胁。

人员威胁分析如图 3-5 所示。

2）系统问题

（1）软件故障。由于系统内部软件发生异常，致使内部公文丢失、损坏、泄密等情况发生，从而对系统安全构成威胁。

（2）硬件故障。由于系统硬件发生故障，致使内部公文丢失、损坏、泄密等情况发生，从而对系统安全构成威胁。

（3）恶意代码。由于用户操作过程中被提交了恶意代码，致使系统内部公文丢失、损

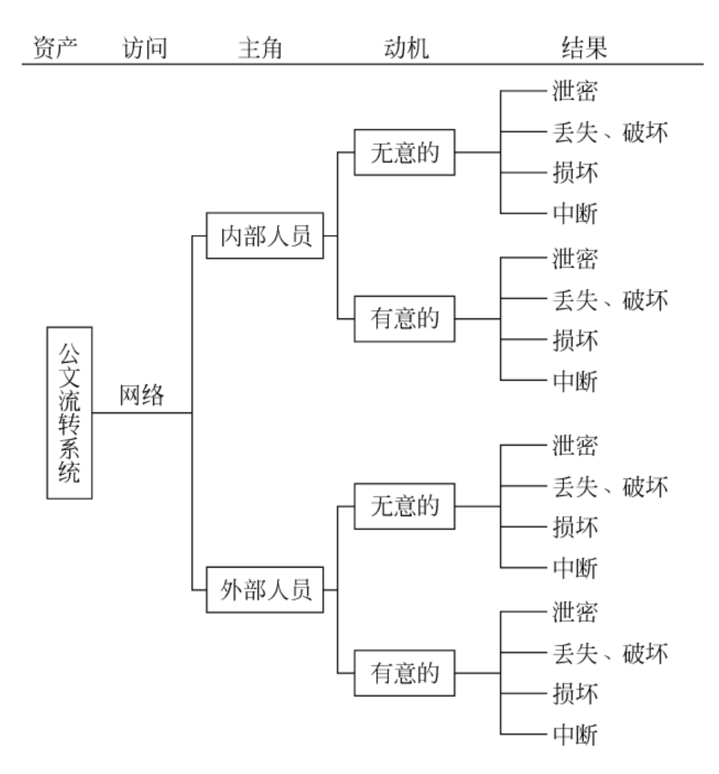


图 3-5 人员威胁分析

坏、泄密等情况发生，从而对系统安全构成威胁。

(4) 系统崩溃。由于系统不稳定引起的崩溃，致使系统内部公文丢失、损坏、泄密等情况发生，从而对系统安全构成威胁。

系统威胁分析如图 3-6 所示。

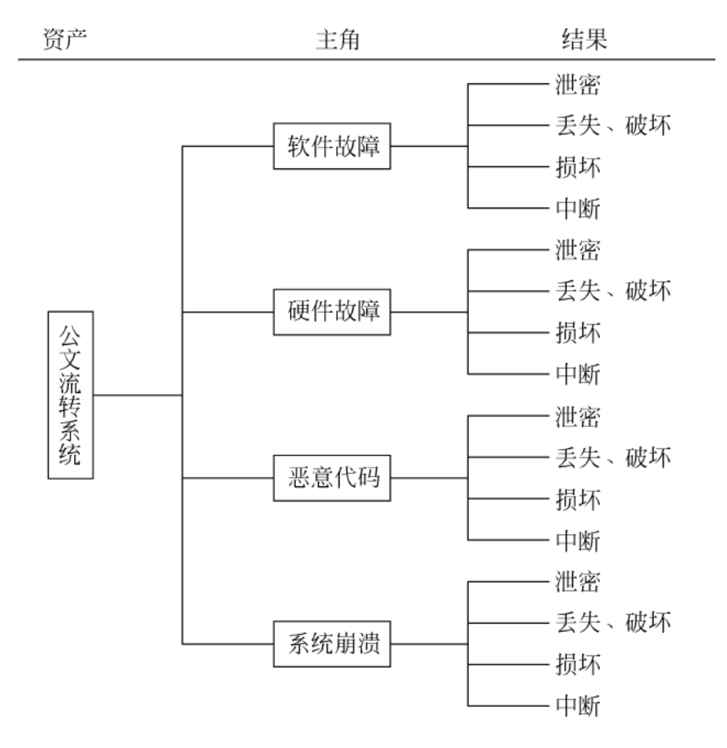


图 3-6 系统威胁分析

3. 确定安全需求

针对威胁分析与威胁分析可能造成的后果,确定了以下安全需求。

(1) 认证需求。提供某个实体的身份认证,保证只有合法用户才能访问到系统内资源。

(2) 访问控制需求。涉密公文必须得到严格的访问控制,确保非法访问者无法访问。

(3) 保密需求。涉密公文必须加密存放、加密传输。

(4) 数据完整性需求。公文必须得到严格的完整性保护,以防止未经授权的增加、删除、修改和代替。

(5) 不可否认需求。公文必须得到严格的防抵赖保护,确保公文的收发都无法抵赖。

(6) 可用性需求。为防止设备故障,软件故障发生引发的一系列问题,对数据进行备份,确保有据可查。

3.3.3 定义信息保护系统

1. 确定信息保护目标

针对以上分析得到的公文流转系统安全需求,本章提出了如下的信息保护目标。

(1) 保密性。信息不能被未授权的个人、实体或者过程利用所获知。

(2) 完整性。保护公文、信息准确和完整。

(3) 可用性。根据授权实体的要求可访问和利用指定的资源。

(4) 真实性。保证主体或资源的确是其所声称的身份、角色。

(5) 可核查性。确保实体行为能被有效跟踪和记录。

(6) 不可否认性。一个已发生的事件可被确认证明,在事后不能否认这个事件或者行为的发生。

2. 信息保护系统功能分析

该信息保护系统应实现对用户的身份认证和访问控制功能,同时应该实现对用户的主要操作进行日志记录,并提供日志审计功能。系统应该通过实现以上安全措施达到对系统中信息的保护,使得系统中的信息具有较强的保密性、不可篡改性和可追溯性。这样,系统中的机密信息才会得以保护,并且即使系统中的信息被非法篡改,也可以通过查阅日志记录追溯到嫌疑人并且对其追究相应的责任,其信息保护功能分析如下。

1) 用户认证功能

由于公文处理工作具有保密性、严肃性的特点,因而公文流转系统必须使用与之相适应的身份认证技术,并基于此形成完备的用户访问控制体系。

该部分功能的实现能满足真实性的信息保护目标。

2) 访问控制功能

访问控制是通过某种途径显式地准许或限制访问能力及范围的一种方法,是针对越权使用系统资源的防御措施;通过限制对关键资源的访问,防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

该部分功能的实现能满足可用性的信息保护目标。

3) 数字签名与传输加密功能

公文流转过程中严格的保密性是公文流转系统基本的要求之一,所以一个成熟的公文流转系统必须使用数字签名技术,并在其基础上对数据传输进行加密。数字签名技术也是识别用户身份,确定公文责任的主要技术。

该部分功能的实现能满足保密性、完整性及不可否认性的信息保护目标。

4）审计功能

通过日志审计系统，企业管理员可以随时了解整个 IT 系统的运行情况，及时发现系统异常事件；另外，通过事后分析和丰富的日志系统，管理员可以方便、高效地对系统进行有针对性的安全审计。遇到特殊安全事件和系统故障，日志审计系统可以帮助管理员进行故障快速定位，并提供客观依据进行追查和恢复。

在公文流转系统中，日志记录主要包括记录用户操作，如登入、查看、审核和修改文件，文件当前的状态，如在审核中、审核完毕、归档等。

该部分功能的实现能满足可核查性的信息保护目标。

3.3.4 设计信息保护系统

根据以上分析，公文流转信息保护系统由四个安全功能模块组成，分别是用户认证模块、访问控制模块、安全审计模块和内容保护模块。每个模块均有各自的功能，负责实现不同的安全服务。并且，各个模块之间相互协调运作，对系统安全的保护起到重要的作用。安全保护系统功能模块如图 3-7 所示。

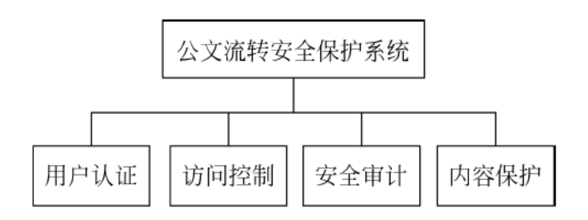


图 3-7 安全保护系统功能模块图

1. 用户认证设计

本系统采用 PKI/CA（Public Key Infrastructure/Certificate Authority）的方式进行用户认证。用户注册后，将从 CA 处获取数字证书。当用户登录时，需提交数字证书进行身份验证。用户身份认证流程如图 3-8 所示。

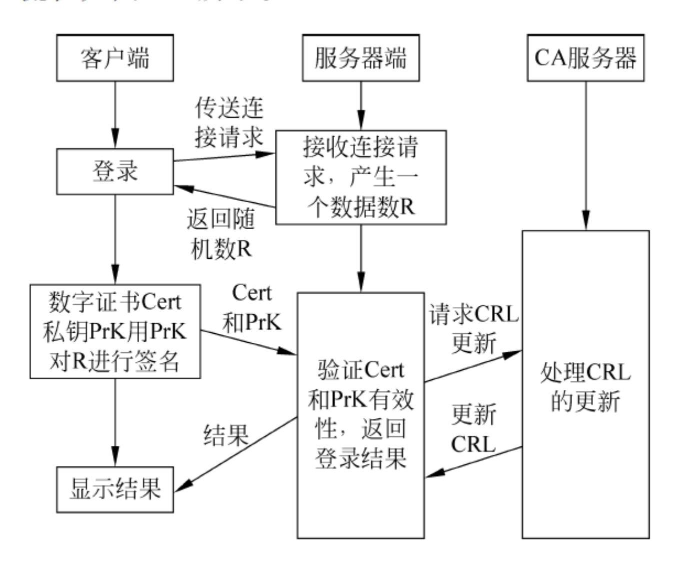


图 3-8 用户身份认证流程

2. 访问控制设计

由于公文流转系统本质上是一种工作流系统，并且一次流转流程中，存在诸多权限不同的用户，使用基于角色的访问控制可以很好地实现。但是基于角色的访问控制(Role-Based Access Control，RBAC)模型对于授权访问是静态的，对动态的公文流转没有良好的解决方法，这里对 RBAC 模型进行扩展。将公文分为静态公文和动态公文，动态公文的访问控制由关系定义进行补充。使用 RBAC 模型和关系约定，可以很好地实现公文流转中的访问控制。

访问控制的主要任务就是保证公文资源不被非法使用和访问，所以所指定的访问控制安全策略应该根据客体的属性而设定。由于客体分为动态客体(即流转中的公文)与静态客体(即归档后公文)，所以安全策略也应该分为动态策略和静态策略。由于在发文管理和收文管理中，其对象主要是动态客体，所以这里设计部分只考虑动态策略的构建。

1) 收文流程

收文是指由办公室进行接收，并指定特定权限的角色传阅。在这个流程中，为了防止公文被篡改，设置所有角色只对公文基本内容有“读”权限。基于角色的权限控制具体策略如下。

(1) 在收文流程中，按照三元组的定义，只有角色(收文员、相关管辖、办公)才享有创建动态公文客体的权限，即首次收文并将公文转入流程系统的权限，并对公文进行初始化如下。

① 当前阶段为“签收”。

② 当前激活区域为公文基本信息(公文编号、公文标题、公文内容等)。

③ 初始化当前控制者。

④ 前处理者为无。

(2) 公文流转阶段的规则。除非处理过程完成，即阶段为“处理”，否则只能按照规定的流程进行流转。如果需要多次交互，则有控制流程权限的用户可以做适当的调整，指定公文流转的下一个用户。这些交互过程由逻辑值决定是否转入新的流转阶段。

(3) 如果当前阶段为 a1，当前控制者为 user1，则当 user1 完成现阶段操作后，将客体向下一个阶段流转时，需要完成以下任务。

① 修改当前阶段的值，并且下一个阶段的值要满足公文流转阶段的规则。

② 设定下一个控制者的角色，并且下一个控制者的角色的值必须满足授权接手公文的角色。

(4) 当用户 user1 成为协办方时，需要完成修改“公文——协办者”关系，将 ID 加入关系中。

(5) 用户 user1 对流转中的公文的访问权限，即具体可执行的基本操作，按照下列策略规定。

① 如果用户为动态客体的“当前控制者”，并已有登记信息，就可以对公文执行当前阶段角色允许的操作；如果用户是“前处理者”，则只对公文的基本信息拥有读的权限；如果用户既不是控制者、协办者，也不是前处理者，则对公文没有任何访问权限。

② 如果角色中有公文反馈权限，则可以将不满意的公文设置相应的逻辑值为 False，并将流程返回给最后一位“前处理者”进行重新批阅，这称作一次交互。交互流转时，其他与交互过程无关的用户只有读权限。

③ 如果当前控制者所处的角色中，有调整流转流程的权限，则可以对公文流转的过程进行自定义规定，同时记录控制信息到公文临时信息中。

④ 当公文处理阶段完成之后，一次收文流程完成，这时，公文转变为静态客体，所有角色对其都只有读权限。

2）发文流程

发文是公文流转系统中又一个重要的部分，通过发文流程，可以完成将动态客体转变为静态客体的过程。具体的访问控制策略与收文流程相同。

（1）在发文流程中，按照角色定义，有角色（起草人、相关管辖、办公）负责发文流转过程中动态公文的创建，并填写公文基本信息、访问信息、临时信息等初始化工作。起草阶段完成后，可以获得一份粗略的动态客体。

（2）由发文流程可知，在发文流转中，不存在收文流程中的交互过程，即不存在动态公文被打回去的情况。

（3）如果当前阶段为 a1，当前控制者为 user1，则当 user1 完成现阶段操作后，将客体向下一个阶段流转时，需要完成以下的任务。

① 修改当前阶段的值，并且下一个阶段的值要满足公文流转阶段的规则。

② 设定下一个控制者的角色，并且下一个控制者的角色的值必须满足授权接收公文的角色。

（4）当用户 user1 成为协办方时，需要完成修改“公文——协办者”关系，将 ID 加入关系中。这时，用户对公文基本内容有读权限，对公文临时信息部分有读写权限。

（5）用户 user1 对流转中的公文的访问权限，即具体可执行的基本操作，按照下列策略规定。

① 如果用户为动态客体的“当前控制者”，并已有登记信息，就可以对公文执行当前阶段角色允许的操作；如果用户是“前处理者”，则只对公文的基本信息拥有读的权限；如果用户既不是控制者、协办者，也不是前处理者，则对公文没有任何访问权限。

② 如果当前控制者所处的角色中，有调整流转流程的权限，则可以对公文流转的过程进行自定义规定，同时记录控制信息到公文临时信息中。

③ 当公文处理阶段完成之后，一次收文流程完成，这时，公文转变为静态客体，所有角色对其都只有读权限。

（6）由发文流程可知，最终文档的整合由办公人员完成，即公文的编号、盖章、发文、归档的授权角色。

（7）当公文归档后，一次发文流转完成，动态公文转换为静态公文，这时，所有角色对静态公文都只有读权限。

3. 安全审计设计

日志是记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。经过规范化、过滤、归并和警告分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统的全面审计。

在公文流转系统中，日志记录主要包括记录用户操作，如登录、查看、审核和修改文件，文件当前的状态，如在审核中、审核完毕、归档等。

1）用户登录

用户登录的日志记录应该包含事件编号、用户名、用户登录 IP 地址、登录是否成功、登

录时间、退出时间、日志类别。

(1) 事件编号。用户登录事件的编号。

(2) 用户名。用户登录名。

(3) 用户登录 IP 地址。用户登录地点的 IP 地址。

(4) 登录是否成功。用户是否登录成功。

(5) 登录时间。用户登录的时间。

(6) 退出时间。用户退出的时间。

(7) 日志类别。日志记录属于哪一个类别。若属于用户类别,则日志记录的是用户登录的事件;若属于文件处理,则记录的是用户处理文件的记录。

用户登录日志如表 3-2 所示。

表 3-2　用户登录日志

事件编号	用户名	用户登录 IP 地址	登录是否成功	登录时间	退出时间	日志类别
0001	Sa	1.1.1.1	是	2018-12-19	2018-12-19	用户
0002	Admin	127.0.0.1	是	2018-12-19	2018-12-19	用户

2) 处理文件

处理文件的日志记录,包含文件编号、文件名、处理人员、处理方式、处理部门、处理时间、日志类别、安全级别。

(1) 文件编号。文件自动进行编号。

(2) 文件名。文件名字。

(3) 处理人员。对文件进行处理的人员。

(4) 处理方式。用户对文件进行的操作,例如收文登记、收文拟办、核签、审核、批示、批复意见填报、收文办理、归档。

(5) 处理部门。对文件进行处理的人员的部门。

(6) 处理时间。文件处理的时间。

(7) 日志类别。日志记录属于哪一个类别。若属于用户类别,则日志记录的是用户登录的事件;若属于文件处理,则记录的是用户处理文件的记录。

(8) 安全级别。分为安全、警告、危险。安全级别表示用户登录操作或文件处理在用户权限之内,没有越权情况发生;警告级别表示用户频繁登录,登录 IP 地址变化频繁,对文件提出异常处理请求或文件处理异常;危险级别表示用户对文件进行越权访问。

用户收文过程日志如表 3-3 所示。

表 3-3　用户收文过程日志

文件编号	文件名	处理人员	处理方式	处理部门	处理时间	日志类别	安全级别
1001	公文 1	办公室 1	处理	办公室	2018-12-1	文件处理	安全
1002	公文 2	主管领导 1	批示	主管部门	2018-12-2	文件处理	安全
1002	公文 2	分管领导 1	审阅	分管部门	2018-12-2	文件处理	安全
1004	公文 4	科员 1	办理	科室	2018-12-3	文件处理	安全
1004	公文 4	办公室 1	登记	办公室	2018-12-5	文件处理	安全

用户发文过程日志如表 3-4 所示。

表 3-4　用户发文过程日志

文件编号	文件名	处理人员	处理方式	处理部门	处理时间	日志类别	安全级别
1001	公文 1	起草人 1	起草	科室 1	2018-12-1	文件处理	安全
1001	公文 1	科员 1	审核	科室 1	2018-12-2	文件处理	安全
1001	公文 1	分管领导	审批	分管部门	2018-12-2	文件处理	安全
1001	公文 1	主管领导	签发	主管部门	2018-12-3	文件处理	安全
1001	公文 1	办公室 1	编号,发文	办公室	2018-12-5	文件处理	安全
1001	公文 1	起草人	结稿	科室 1	2012-12-4	文件处理	安全

3）日志文件的保护

日志文件的查看权限：需要管理员权限才可查看日志记录文件；日志文件的修改和删除应设置为本地管理员登入才可处理。

4. 内容保护设计

公文流转过程中，主要有三种情况的文件传送。

（1）一对多的公开明文发送。只需要以明文的方式发送公文，如校长办公室发送给全校的放假通知。

（2）多对一的公文发送。如下级部门的公文，需要发给上级签字。公文需要以密文的方式发送，并且需要保证公文被正确的人签字。

（3）一对一的公文发送。如领导发送给各部门主管的重要通知，必须以密文形式发送，以免被他人截获，从而泄露公司秘密。

此案例采用非对称密码体制来保证公文内容的安全。

3.3.5 实施信息保护系统

基于 ISSE 的设计理念，可以将公文流转系统的实施部分划分为 3 个模块，如图 3-9 所示。

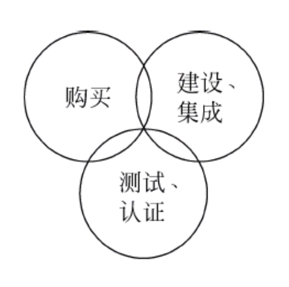


图 3-9　实施信息保护系统的 3 个模块

1. 购买

根据系统设计部分的要求，购买搭建公文流转系统所必需的服务器设备（网站服务器、数据库服务器、VPN 设备），硬件防火墙，路由器等。如有必要，相应的软件服务也需购买。

2. 建设、集成

根据系统设计部分的各个模块需求，集成收文管理和发文管理的两大基本功能。其中收文管理集成了收文登记、收文拟办、核签、审核、批示、批复意见填报、收文办理、归档等功能；发文管理集成了文件拟稿、文件复核、主管领导复核、领导签发、经办人分发传阅、文件归档等功能。最终建设出具备用户认证和访问控制功能，同时对用户的主要操作具备日志记录和日志审计功能的公文流转系统。

3. 测试、认证

按照 ISSE 的标准测试所构建的公文流转系统能否满足用户需求，是否具备用户认证和访问控制功能，是否具备对用户的主要操作有日志记录和日志审计的功能，且能满足用户和认证员的要求。

3.3.6 评估信息保护有效性

该项目主要是实现公文流转系统上的用户验证、访问控制、信息保密性、数据完整性、不可否认性、建立起一套完善的公文流转系统安全保障体系。评估信息保护的有效性主要集中于该信息保障系统的有效性，即系统在保密性、完整性、可用性、不可否认性等安全特性方面的有效性。

项目主要从 5 个方面进行了有效性评估。

1. 实体鉴别

登录系统的用户需要通过身份认证，只有合法的用户才可以访问系统，执行操作。而系统也要提供系统证书，防止有第三者假冒系统。

2. 权限控制

用户新建公文或者审核公文的时候，都需要相应的权限验证，确保该用户有权力访问所要求的公文，进行所要求的操作。

3. 数据保密性

保证公文在前一环节的用户到下一环节之间的传输不被窃听，只有指定的用户才能阅读指定的公文。只有的得到文件服务器的权限才可以访问文件服务器。

4. 不可否认性

公文的提交方不能否认在公文上载明的时间提交过这份公文，接受方不能否认在载明的时间接受过该公文。

5. 数据完整性

公文在传输过程不被插入、修改、更改顺序或者重放。

3.4 小　　结

总的来说，信息系统安全工程规定了在各个阶段应该达到的目的，但没有规定具体的工具和方法，只是从系统论的角度指明了一个框架和范围，实施的细节依赖于已有的经验和积累。信息系统安全工程沿袭了系统工程以时间维划定工程元素的方法学，暴露出一些不足。首先，很多安全要求应该贯彻在整个工程过程之中，尤其是信息安全的保证要求，而信息系统安全工程对其缺乏有针对性的讨论。其次，信息安全的内容极其庞杂，一次完整的信息安全工程过程，往往会涉及多个复杂的安全领域，而有些领域的时间过程性却不明显，以时间维为线索的描述方式不适合反映这些内容。因此，后来在信息安全工程方法的发展上，出现了第二种思路：过程能力成熟度的方法。

习　题

1. 如何发掘信息系统的安全需求？
2. 简述信息系统安全工程的过程。
3. 试比较 ISSE 与 SE。
4. 什么是威胁？一个普通的信息管理系统经常面临什么样的威胁？

第 4 章　SSE-CMM

本章学习目标：

- 了解 SSE-CMM 的基本概念。
- 掌握 SSE-CMM 的过程域。
- 掌握 SSE-CMM 能力级别。

4.1　CMM

4.1.1　CMM 简介

软件能力成熟度模型(Capability Maturity Model,CMM)是卡内基梅隆大学软件工程研究院(Software Engineering Institute,SEI)为了满足美国联邦政府评估软件供应商的要求,于 1986 年开始研究的模型,并于 1991 年推出其 CMM1.0 版,1993 年推出 CMM1.1 版。

CMM 将软件组织的过程能力分为 5 个成熟度级别,每一个级别定义了一组过程能力目标,并描述了要达到这些目标应该采取的实践活动。软件组织通过努力一步步达到这些预定的目标,从而得到持续的过程改进,实现组织高效率、低成本地交付高质量软件产品的战略目标。

CMM 自问世后备受关注,在一些发达国家和地区得到了广泛的应用,成为衡量软件公司组织管理软件产品及开发能力的事实上的工业标准,并为软件公司改善其生产过程提供了重要依据。

4.1.2　CMM 的体系结构

持续的过程改进是许多小的、循序渐进的改进步骤,而不是革命性的变革。CMM 提供了一个框架,将这些渐进的步骤组织成 5 个成熟度的级别,为持续的过程改进奠定了基础。5 个成熟度级别定义了度量组织软件过程和评估软件过程能力的尺度,是一个良好定义并呈螺旋式上升的阶梯形层次结构。CMM 模型的 5 级阶梯式结构,即 CMM 的 5 个能力成熟度等级,如图 4-1 所示。

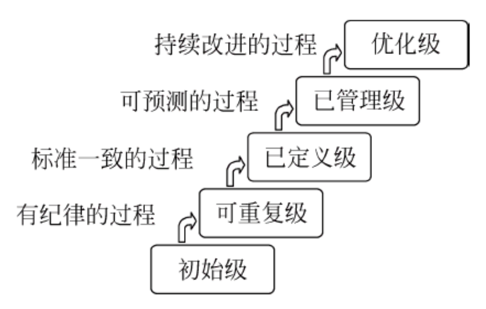


图 4-1　CMM 的 5 个能力成熟度等级

CMM 的各个级别都建立了一组关键过程域(Key Process Area,KPA),这些 KPA 定义了一组过程目标,对软件工程的过程能力提出了明确的要求。如果满足了这组目标,则说明软件过程的某些重要活动已经稳定。随着成熟度级别的上升,目标要求也逐步提高,促使组织有计划、有系统地走向更加成熟和完善。

(1) 第 1 级(初始级)。这时的软件组织没有任何对质量和过程的管理,软件的开发和生产处于无序的状态,产品的成功完全依赖于个人的智慧和努力。

(2) 第 2 级(可重复级)。对基本的项目过程建立了成本、进度和功能实现情况的跟踪管理,建立了一些过程规律和训练。一些重要的过程可以重用以前类似项目的成功经验和结果。

(3) 第 3 级(已定义级)。软件过程的管理和工程活动都已形成标准,并以文件的形式确定下来,成为组织的标准软件过程。所有项目的开发和维护活动都必须遵循这些已被证明的、制度化的软件过程标准,但可以视项目的具体特征,根据制度化的裁减准则进行裁减。

(4) 第 4 级(已管理级)。组织对软件产品和过程都建立了量化的质量目标。一些重要的软件质量活动的生产能力和质量都可按照组织定义的度量程序进行度量,从而使软件项目的计划和估计更加准确。

(5) 第 5 级(优化级)。组织有良好的方法识别过程的缺陷,并采取有效的措施来避免缺陷的非预期或重复发生。第 5 级的组织可以收集有效的软件过程数据,通过对数据的度量,分析新技术的成本效益,并对软件过程改进提出适当的建议。建立良好的技术变化管理机制,促使最好的软件工程实践的革新思想脱颖而出,并辐射到整个组织,使组织的软件过程得到持续的改进和完善。

可见,CMM 的成熟度等级是逐步提高的,每一个级别都有明确的目标集合,每提高一个等级,软件过程就更加成熟。

4.2 SSE-CMM 概述

4.2.1 SSE-CMM 的概念

SSE-CMM 是系统安全工程能力成熟度模型(System Security Engineering Capability Model)的英文缩写,由能力成熟度模型(CMM)发展而来,是以工程域维和能力维来诠释信息安全工程过程的方法学,SSE-CMM 的一个重要用途是对信息安全工程能力进行评估。

SSE-CMM 起源于 1993 年 4 月美国国家安全局(National Security Agency,NSA)对当时各类能力成熟度模型(CMM)工作状况的研究,以判断是否需要一个专门应用于安全工程的 CMM。在这个构思阶段,确定了一个初步的安全工程 CMM 作为这个判断过程的基础。1995 年 1 月,各界信息安全人士被邀请参加第一届公开安全工程 CMM 工作研讨会,来自 60 多个组织的代表肯定了这种模型的需求。由于信息安全业界的兴趣,会议成立了项目工作组,这标志着安全工程 CMM 开发阶段的开始。项目工作组的首次会议于 1995 年 3 月举行。通过 SSE-CMM 指导组织、创作组织和应用工作组织的工作,完成了模型和认定方法的工作。1996 年 10 月发布了 SSE-CMM v1.0 版本,1997 年 4 月制定了 SSE-CMM 评定方法的 1.0 版本,1999 年 4 月,形成了 SSE-CMM v2.0 和 SSE-CMM 评定方法 v2.0,2002 年

3月,SSE-CMM得到了ISO的采纳,成为ISO的标准——ISO/IEC 21827,冠名为《信息技术-系统安全工程-能力成熟度模型》。

SSE-CMM描述了一个组织的安全工程过程的重要特性。为了确保安全工程的良好性,这些特性是完善安全工程的保证,也是信息安全工程实施的度量标准,同时还是一个易于理解的评估系统安全工程的框架。尽管SSE-CMM没有基于时间维规定一个特定的过程和步骤,但是它汇集了信息安全界普遍使用的信息安全工程实施方法。

SSE-CMM是安全工程实施的标准化评估准则,包含了如下内容。

(1) 整个生命周期。包括工程开发、运行、维护及淘汰等。

(2) 整个组织。包括管理、组织和工程活动。

(3) 与其他学科的紧密联系。包括系统、软件、硬件、人类活动和测试工程、系统管理、运行和维护等活动。

(4) 与其他组织的相互联系。包括信息获取、系统管理、产品认证、可信度评估等。

用户和安全产品提供商都非常关注和重视安全产品、安全系统及安全服务的改进。尽管安全工程领域存在着一些普遍公认的原则,但是缺乏一个全面的框架去评估工程实践。系统安全工程能力成熟度模型正是这样一个框架,它为安全工程原则的应用提供了一个衡量和改进的途径。SSE-CMM的目的就是推动安全工程成为一个明确的、成熟的和可衡量的工程活动。具体而言,制定SSE-CMM模型和评价方法的目的如下。

(1) 工程组把投入集中在安全工程工具、培训、过程定义、管理措施及其改进活动上。

(2) 实现基于能力的保证,即信任度是基于一个成熟工作组织的安全实施和过程的可信度。

(3) 可以通过评估投标人的能力水平和相关方案的风险来选择合格的安全工程供应商。

SSE-CMM模型中最重要的术语以及它们在该模型中的含义如下。

1. 过程

过程是指为达到某一个特定目的而执行的一系列活动,这些活动可以重复、递归和并发地执行。从"过程"派生出来的有关术语有"充分定义的过程""已定义的过程"和"执行过程"。充分定义的过程包括对每个活动的定义、每个活动输入的定义和控制活动执行机制的定义。已定义的过程就是被组织正式描述的过程,也是该组织在其安全工程中要使用的过程。执行过程是安全工程师们实际在执行中的过程,它指明安全工程师实际在做什么。

2. 过程域

过程域是由一些基本实施组成的活动范围,它们共同实施来达到一个规定的目标。这些基本实施是强制性的,因为只有它们全部成功地得到执行,才能满足过程域规定的目标。SSE-CMM包含工程、项目和组织3类过程域。组织类与项目类过程域的差别仅仅是所有权不同,项目过程只针对一个特定的产品,而组织过程域则含有一个或多个项目。

3. 工作产品

SSE-CMM中的工作产品是指在执行任何过程中产生出的所有文档、报告、文件和数据。

4. 过程能力

过程能力是通过跟踪一个过程能达到期望结果的可量化范围。一个组织的过程能力可帮助组织预见项目达到目标的能力。位于低能力级组织的项目在达到预定的成本、进度、功能和质量目标上会有很大的变化，而位于高能力级组织的项目则完全相反。

4.2.2 SSE-CMM 体系结构

SSE-CMM 体系结构设计的目标是清晰地从管理和制度化特征中分离出安全工程的基本特征。SSE-CMM 模型采用了两维的结构，即域维（domain）和能力维（capability）。

横轴的域维定义了安全工程的所有实施活动。SSE-CMM 模型将各种各样的系统安全工程任务抽象为 11 个有明显特征的子任务，而完成其中一个子任务所需要实施的一组工程实践称为一个过程域（Process Area，PA），这些 PA 可能出现在安全系统生命周期的各个阶段。SSE-CMM 模型为每个过程域定义了一组确定的基本实施（Basic Practice，BP），并规定每一个基本实践对完成该子任务都是不可缺少的，其组成结构如图 4-2 所示。

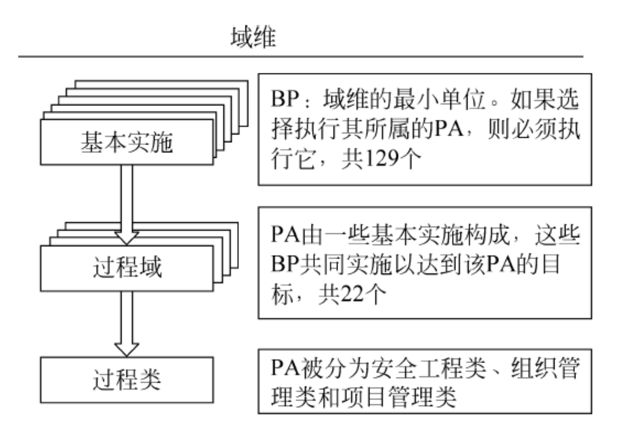


图 4-2 SSE-CMM 域维

纵轴的能力维代表组织能力，它由过程管理与制度化能力构成。在能力维上，模型设置了 6 个能力成熟级别，每个能力成熟级别由一组能反映过程能力变化的公共特征（Common Feature，CF）来定义，这些 CF 适用于所有的 PA，而每一个 CF 又可以由若干项通用实施（Generic Practice，GP）来描述。只有某种级别的所有公共特征都得以实现，才说明该过程区达到了相应的能力级别，其组成结构如图 4-3 所示。

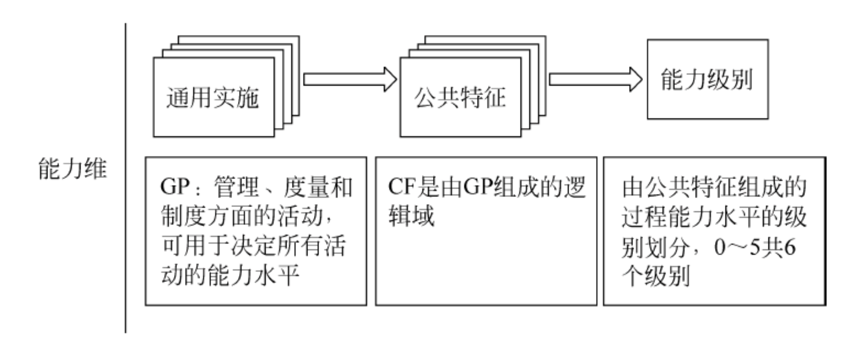


图 4-3 SSE-CMM 能力维

通过设置这两个相互依赖的维，SSE-CMM 在各个能力级别上覆盖了整个安全活动范围。例如安全工程的基础部分是识别安全脆弱性，如图 4-4 所示，该活动在 SSE-CMM 中归于基本实施识别系统安全脆弱性。而确定一个组织是否有能力完成某项活动的方法之一，就是检查它是否有为申明要做的活动配置资源的过程。成熟组织具备的该“特征”，在 SSE-CMM 通用实施中称为“配置资源”。将基本实施和通用实施综合起来，为检查组织完成特定活动的能力提供了一种方法。如有意的一方可能问：“你们组织为识别系统安全脆弱性配置了资源吗?”得到的答案便对组织的能力的初步了解。回答全部基本实施和通用实施相结合而提出的所有问题(交叉点)，就能得到该组织安全工程能力的概貌。

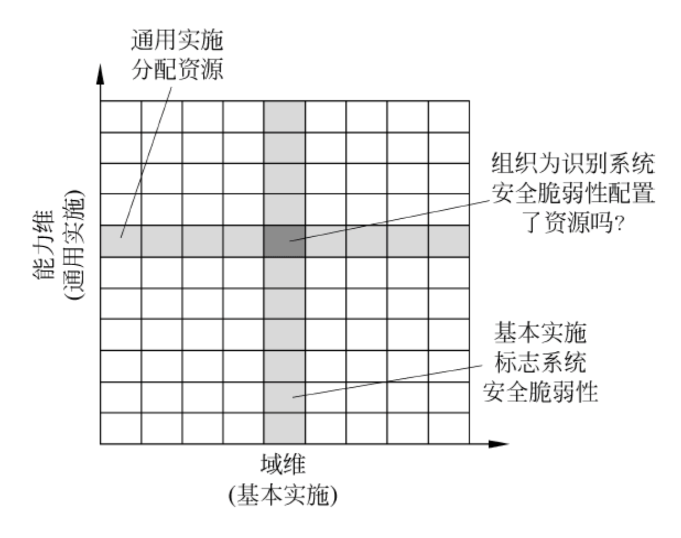


图 4-4　SSE-CMM 两维模型

通过设置这两个相互依赖的维，SSE-CMM 在各个能力级别上覆盖了整个安全活动范围。给每个 PA 赋予一个能力级别评分，所得到的两维图形便形象地反映了一个工程组织整体上的系统安全工程能力成熟度，也间接地反映了其工作结果的质量及其在安全上的可信度，安全过程区域的能力级别评分如图 4-5 所示。

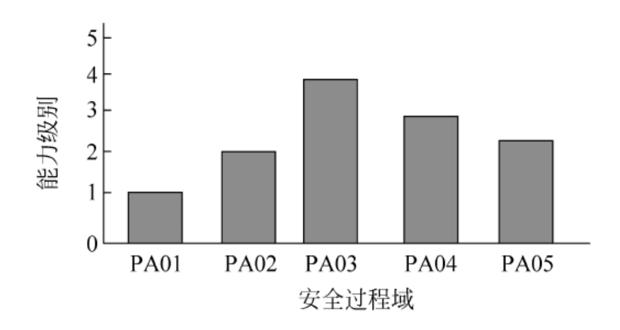


图 4-5　安全过程域的能力级别评分

4.2.3　SSE-CMM 的应用

SSE-CMM 可以用作改进组织安全工程过程的工具，这方面，SSE-CMM 建议采用 SEI 的 IDEAL 模型(Initiating，Diagnosing，Establishing，Acting，Learning)。

(1) Initiating(启动)。目的是进入一个评估当前状况、改进、重复的持续循环之中。熟悉项目目标和完成方式，开发业务案例和项目执行方法，获得管理层批准和支持，为成功地

改进努力做好铺垫。

(2) Diagnosing(诊断)。是理解组织当前和期望的过程成熟度状态,这些是形成组织过程改进行动计划的基础。

(3) Establishing(建立)。是基于努力目标和诊断阶段开发的建议来制订详细的行动计划,计划必须考虑到各种约束。

(4) Acting(操作)。即实施阶段,无论是资源还是时间,都需要各方面付出最大程度的努力。

(5) Learning(学习)。既是本次循环的终止,又是下一次改进过程的开端,对整个过程改进活动进行评估。

对于整个系统工程来说,SSE-CMM 的任务是在评估了系统工程能力之后,将焦点集中在组织的安全工程过程上。结合系统工程能力评估,SSE-CMM 评估可以适当裁减,与 SE-CMM 集成在一起。当不依赖于系统工程能力评估时,SSE-CMM 评估必须考虑到是否有合适的项目和组织基础为安全工程过程提供支持。

4.3 SSE-CMM 的过程域

4.3.1 SSE-CMM 过程域的分类

SSE-CMM 模型中定义了 22 个安全方面的过程域,按照解决问题的不同,过程域分为 3 类:工程过程域(11 个过程)、项目工程域(5 个过程)、组织过程域(6 个过程)。

工程过程域的 11 个过程描述了系统安全工程中实施的与安全直接相关的活动。

(1) PA01 管理安全控制。

(2) PA02 评估影响。

(3) PA03 评估安全风险。

(4) PA04 评估威胁。

(5) PA05 评估脆弱性。

(6) PA06 建立保证论据。

(7) PA07 协调安全性。

(8) PA08 监视安全态势。

(9) PA09 提供安全输入。

(10) PA10 确定安全需求。

(11) PA11 验证与确认安全。

组织和项目过程类中包含 11 个过程,并不直接同系统安全相关,但常与 11 个工程过程一起用来度量系统安全队伍的过程能力成熟度。其中,PA12～PA16 是项目过程,PA17～PA22 是组织过程。

(1) PA12 保证质量。

(2) PA13 管理配置。

(3) PA14 管理项目风险。

(4) PA15 监视和控制技术活动。

(5) PA16 计划技术活动。

(6) PA17 定义组织的系统工程过程。

(7) PA18 改进组织的系统工程过程。

(8) PA19 管理产品系列进化。

(9) PA20 管理系统工程支持环境。

(10) PA21 提供持续发展的技能和知识。

(11) PA22 与供应商协调。

4.3.2　工程过程域

工程过程域分为 3 个基本类别的领域：风险过程、工程过程和保证过程，如图 4-6 所示。尽管这 3 个域并不是相互独立的，但还是需要将它们区分开来。就最简单的层次而言，风险过程要识别内含与产品以及系统开发过程中的危险因素，并将其按危险性的等级进行排列；工程过程则要对上述危险带来的问题采取解决措施；保证过程则要确保有效的安全解决措施，并将这种措施传递给客户。这 3 个域同时协作，才能实现安全工程所要达到的目标。

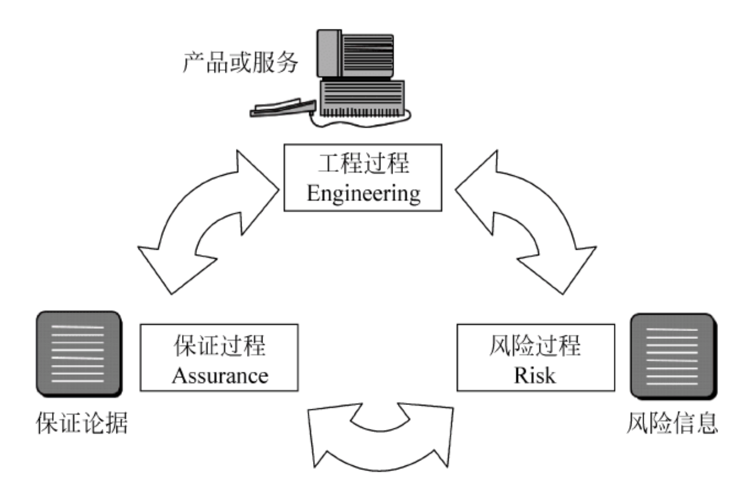


图 4-6　安全工程过程域的 3 个基本域

1. 风险过程

安全工程中的一个核心目标就是降低风险。降低风险需要不断地进行风险评估，发现潜在的问题。风险评估往往从这两个方面考虑：第一，系统受到攻击时崩溃的可能性大小；第二，一些意外的事件对系统的影响。上述可能性是一个不确定因素，它会随着环境的改变而改变，这就意味着这种可能性只能用某种极限的形式进行预测。另外，由于意外事件并不一定总是如意料中的那样发生，这就决定了所考虑的特殊风险对系统的影响也是一个不确定因素。由于这些因素都含有大量的不确定性，这就致使准确估计这些因素成为一件非常困难的事情。

采取安全防范措施可以降低风险，但是这种防范措施本身也可能带来风险。通常而言，要彻底根除所有风险是不可能的，一方面是由于降低风险措施所增加的大量费用，另一方面是由于风险本身具有很强的不确定性。正因为这样，一些参与风险总是必须被接受。在高度不确定的环境下，接受风险将会带来很多问题。

与风险过程相关的过程如图 4-7 所示。

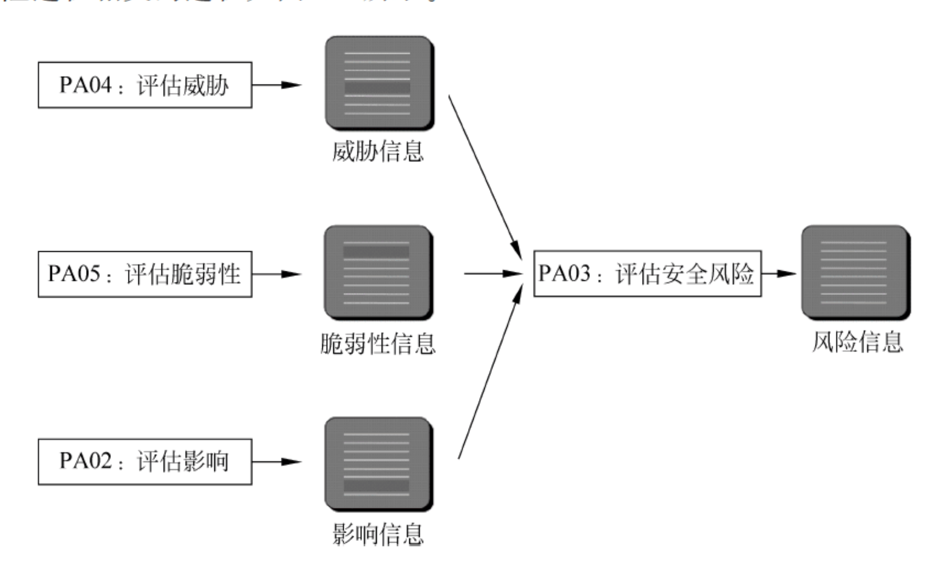


图 4-7　与风险过程相关的过程

1）PA02：评估影响

评估影响的目的在于识别系统可能受到的影响，并评估这些影响发生的可能性。影响可能是有形的，例如税收或财政罚款的损失；也可能是无形的，例如声誉和信誉的损伤。目标是为了确定并描述风险可能对系统带来的安全影响。

（1）基本实施列表。

① BP02.01。标识、分析系统的运行、业务或任务功能，并对这些功能的优先级进行排序。

② BP02.02。对支持系统的关键性运行能力或安全目标的系统资产进行标识和描述。

③ BP02.03。选择可用于评估的影响度量准则。

④ BP02.04。对评估中使用的度量准则与所需的转换因子（如果需要）之间的关系进行确定。

⑤ BP02.05。标识和描述影响。

⑥ BP02.06。监视影响的不断变化。

（2）说明。

① BP02.01。对功能进行优先级排序，用来对机构的运行、业务或任务功能进行标识、分析和优先级排列，还应考虑到业务战略可能受到的影响。这些行为将会影响和缓解一个机构可能遭受的影响，也会继而对其他过程域中的风险评估工作产生影响。

② BP02.02。标识系统资产，标识出系统中为支持系统安全目标或关键功能（运行功能、业务功能或任务功能）所必需的资源和数据。该基本实施可以通过评估各类资产在给定环境中（对安全目标或关键功能提供支持）的重要性来定义出各类资产。

③ BP02.03。选择影响的度量规则。有很多度量准则可用于衡量事件的影响。在评估之前，应预先确定采用何种度量准则来评估具体系统面临的影响，选择影响的度量准则。

④ BP02.04。确定不同度量准则之间的关系。某些影响可能需要使用不同的度量准则进行评估，因此必须确定不同度量准则之间的关系，以确保在整个影响评估中使用一致性的方法对所有影响进行评估。在某些情况下，还需要将各种度量准则组合起来，以产生唯一的确定性结果。

⑤ BP02.05。标识和描述影响。利用 BP02.01 和 BP02.02 中确定的资产和功能信息来确定安全事件的可能影响。对每一项资产来说，这种影响可能包括资产的破坏、泄露、阻断或丢失。功能的影响可能包括拦截、延迟、弱化。一旦创建了相对完整的影响列表，便可以用 BP02.03 和 BP02.04 中确定的度量准则或度量准则的组合来描述影响，其中可能还要参考机构的保险情况、财政年检等。在评估中，要考察其中的不确定性，并与影响相联系。

⑥ BP02.06。监视影响。任何位置和状态下的影响都是动态变化的。新的影响可以变成互为关联。因此，需要监视现有影响并有规律地检查可能的新影响。该基本实施与 BP08.02 中的通用性监视活动紧密相连。

2）PA03：评估安全风险

评估安全风险的目的在于标识出一给定环境中某一系统的安全风险。这一过程域将基于机构的功能和资产在面对威胁所表现出的脆弱性的理解而确定系统的安全风险。该工作特别涉及对安全事件“暴露”的可能性进行标识和评估。“暴露”一词指的是可能对系统造成重大伤害的威胁、脆弱性和影响的组合。在系统生命周期的任何时候都可进行这一系列活动，以便对已知环境中的系统的开发、维护和运行做出决策。

（1）基本实施列表。

① BP03.01。选择用于分析、评估和比较给定环境中系统安全风险依据的方法、技术和准则。

② BP03.02。标识威胁/脆弱性/影响三组合（暴露）。

③ BP03.03。评估与每个暴露相关的风险。

④ BP03.04。评估与风险相关的总体不确定性。

⑤ BP03.05。排列风险的优先顺序。

⑥ BP03.06。监视风险及其特征的不断变化。

（2）说明。

① BP03.01。选择风险分析方法，定义用于标识一给定环境中系统安全风险的方法，以对安全风险进行分析、评估和比较。它还包括一个对风险进行分类和分级的方案。

② BP03.02。标识暴露。标识威胁、脆弱性、影响的三组合（暴露）。标识暴露的目的在于认识这些威胁和脆弱点的利害关系，进而标识威胁和脆弱性造成的影响。这些暴露是选择系统保护措施时必须考虑的。

③ BP03.03。评估暴露的风险，标识出每一个暴露的可能性。

④ BP03.04。评估总体的不确定性。每种风险都有与之相关的不确定性。总体的风险不确定性是在 BP04.05 评估威胁的可能性、BP05.03 收集脆弱性数据、BP02.05 标识和描述影响中标识的不确定性的累积。本实施过程与 PA06 建立保证论据联系紧密，因为保证能用于改变（很多时候是减低）不确定性。

⑤ BP03.05。排列风险优先级。已经标识的风险应该基于机构的优先安排、风险出现的可能性、与这些因素相关的不确定性以及可用的财力而进行排序。风险可以被减轻、规避、转移或接受，也可以使用这些措施的组合。

⑥ BP03.06。监视风险及其特征。任何位置和状态下的风险都是动态变化的。新的风险可能出现，现有的风险也会发生变化。因此，需要有规律地监视现有风险及特征，并检查可能的风险。该基本实施与 BP08.02 中的通用性监视活动紧密相连。

3）PA04：评估威胁

评估威胁过程域的目的在于标识安全威胁及其性质和特征。对系统安全的威胁进行标识和描述。

（1）基本实施列表。

① BP04.01。标识由自然因素所引起的威胁。

② BP04.02。标识由人为因素所引起的无意或有意的威胁。

③ BP04.03。标识在一特定环境中的测量单元和适用范围。

④ BP04.04。评估由人为因素引起的威胁主体的能力和动机。

⑤ BP04.05。评估威胁事件出现的可能性。

⑥ BP04.06。监视威胁以及威胁特征的变化

（2）说明。

① BP04.01。标识自然威胁，有自然原因引起的威胁包括地震、海啸和台风等。然而，并非所有的自然威胁都会在所有地方发生。因此，重要的是标识出在一具体地方到底会存在哪一种自然威胁。

② BP04.02。标识人为威胁，认为原因引起的威胁与自然威胁不一样。它基本有两种类型：偶然原因引起的威胁和故意原因引起的威胁。在某些环境中，因为不涉及人为威胁，可以在经过分析后取消对人为威胁的考察。

③ BP04.03。标识威胁的测量单元。大量的自然和人为威胁都有其与之相关的测量单元。例如地震的里氏震级。大多数情况下，测量单元的全部尺度并不适用于一次具体的评估。因此，对可能在一个机构中出现的事件，可根据具体情况建立最大和最小测量单元。

④ BP04.04。评估威胁主体的能力，确定可能对系统发动攻击的敌人的主观能力和客观能力。主观能力是指一个攻击者所掌握的攻击知识（例如经过的训练和拥有的技能）；客观能力是指一个有能力的敌人实际发动攻击的可能性（例如拥有的资源）。

⑤ BP04.05。评估威胁的可能性，对威胁事件发生的可能性进行评估。在评估中需要考虑多种因素，从自然事件的概率到人员的有意或无意行为的概率等均可能需要评估。并不是说这些所有因素都要去计算或测量，但这其中应该有一个一致的度量准则。

⑥ BP04.06。监视威胁及其特征。任何位置和状态下的威胁都是动态变化的。新的威胁可能出现，现有的威胁也会发生变化。因此，需要有规律地监视现有威胁及特征，并检查可能的新威胁。该基本实施与 BP08.02 中的通用性监视活动紧密相连。

4）PA05：评估脆弱性

评估安全脆弱性的目的在于标识和描述系统的安全脆弱性。本过程域包括分析系统资产、定义具体的脆弱性以及对整个系统的脆弱性进行评估。与安全风险和脆弱性评估有关的术语，在许多不同场合的使用是不同的。就本模型的用途而言，“脆弱性”指的是可被利用完成不期望行为的系统的某些特征、安全弱点、漏洞或易被威胁所攻击的系统实施的缺陷。这些脆弱性与任何特定的威胁或攻击的形成并不关联。本过程域的活动在系统生命周期内任何时间都可进行，以支持在已知环境中系统的开发、维护和运行决策。目标是获得对一给定环境中系统安全脆弱性的理解。

（1）基本实施列表。

① BP05.01。选择对一给定环境中的系统脆弱性进行标识和描述的方法、技术和

标准。

② BP05.02。识别系统安全脆弱性。

③ BP05.03。收集与脆弱性属性有关的数据。

④ BP05.04。评估系统脆弱性并将特定脆弱性及各种特定脆弱性的组合结果进行综合。

⑤ BP05.05。监视脆弱性的变化及其特征的变化。

(2) 说明。

① BP05.01。选择脆弱性分析方法,包括定义系统的脆弱性分析方法,以对安全脆弱性进行标识和描述,其中还包括脆弱性的分类和优先级排序方案,以威胁及其可能性、系统的运行功能、安全需求或其他为基础来完成脆弱性的分类和排序。

② BP05.02。标识脆弱性,记录系统脆弱性。

③ BP05.03。收集脆弱性数据。脆弱性有自身的属性,该基本实施旨在收集与这些属性有关的数据。标识和收集脆弱性被利用的难易程度、脆弱性存在的可能性等数据。

④ BP05.04。综合系统的脆弱性,分析那些脆弱性或脆弱性的组合给系统带来的问题。分析中还应确定该脆弱性的属性特征,例如脆弱性被利用以及被成功攻击的概率,并提出脆弱性的综合分析建议。

⑤ BP05.05。监视脆弱性及其特征。任何位置和状态下的脆弱性都是动态变化的,新的脆弱性可以从中产生,现有的脆弱性的特征也会发生变化。因此,需要有规律地监视现有脆弱性及特征,并检查可能的新脆弱性。该基本实施与 BP08.02 中的通用性监视活动紧密相连。

2. 工程过程域

与其他工程标准一样,安全工程也是一个包括概念、设计、实施、部署、维护、更新等多个环节的过程。SSE-CMM 强调,安全工程师是整个团队中非常重要的一个部分,必须与其他团队紧密合作,这样才能有助于使安全性成为整个大过程中的一部分而不是仅作为一个孤立的活动。安全工程师在确定安全需求时要用到多方面的信息,包括风险过程中产生的信息,以及其他关于系统需求、相关法律、政策等多方面的信息。在确定了安全需求后,安全工程师将针对安全需求提出一系列的安全解决措施。解决措施的过程一般包含两方面工作:首先确定可能的代替方案;然后评估替代方案,以决定哪一个方案更合适。将这种过程与其余活动相集成时存在一个难点:解决措施的选择不能仅着眼于安全考虑,而应该考虑更广泛的因素,包括费用、执行情况、技术风险以及使用的便易性。通常这种决策必须要将问题再次发生的可能性降至最低,这一步骤中产生的分析结果将为以后的安全保证工作打下一个坚实的基础。

与工程过程相关的过程如图 4-8 所示。

1) PA01:管理安全控制

管理安全控制的目的在于确保已集成到系统设计中的预期的系统安全性确实能够在最终系统运行状态中实现。

(1) 基本实施列表。

① BP01.01。建立安全控制的职责和可追究性,并通知到机构中的每一个人。

② BP01.02。管理系统安全控制的配置。

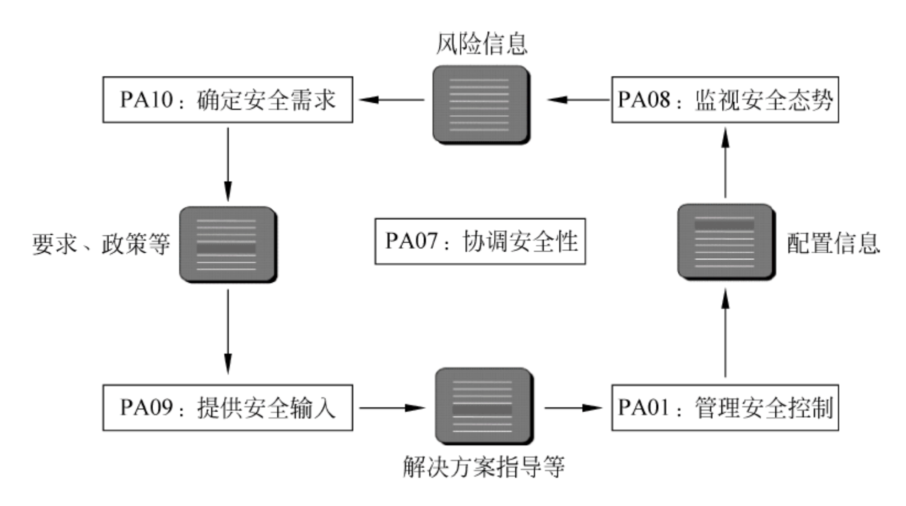


图 4-8　与工程过程相关的过程

③ BP01.03。管理所有的用户和管理员的安全意识、培训和教育项目。

④ BP01.04。对安全服务及控制机制的定期维护和管理。

(2) 说明。

① BP01.01。建立安全职责，本过程应确保安全责任人员的行为能够得到追踪(即可追究性)，并授予安全责任人相应的行动与权力。同时也应该确保所采用的所有安全控制是明确的并且一致性的应用。此外还应该确保所采纳的安全管理结构，不但要通知管理层内的所有人，而且也应通知整个机构。

② BP01.02。管理安全配置，所有设备的安全配置需要管理。由于系统安全很大程度上依赖于许多相关组件(硬件、软件与程序)，而常规配置管理实施不必关心安全系统所需的互相关联性。

③ BP01.03。管理安全意识培养、培训和教育项目，所有员工的安全意识培养、培训和教育都需要管理，其管理方式与其需要管理的意识、培训和教育管理方式相同。

④ BP01.04。管理安全服务及控制机制，安全服务及机制的一般管理类似于其他服务及机制的管理，这包括保护它们避免破坏、偶然事故和人为故障，并与法律和政策要求一致。

2) PA07：协调安全性

协调安全的目的在于保证所有团体都有一种参与安全工程活动的意识，并确实能够参与到安全工程活动中。由于安全工程不能独立地取得成功，所以这种参与工作是至关重要的。这种协调涉及要保持所有项目人员与外部团体之间的开放交流。多种机制可以用于在这些团体之间协调和沟通安全工程的决策和建议，包括备忘录、文档、电子邮件、会议和工作组。

(1) 基本实施列表。

① BP07.01。定义安全工程协调目标和相互关系。

② BP07.02。标识出安全工程的协调机制。

③ BP07.03。促进安全工程的协调。

④ BP07.04。用标识出的机制去协调有关安全的决策和建议。

(2) 说明。

① BP07.01。定义协调目标，许多团体需要有一种参与安全工程的意识，并参与到安

全工程活动中。要通过检查项目结构、信息需求和项目要求来决定与这些团体共享信息的目标。建立与其他团体之间的联系和承诺(义务关系)。成功的联系可有许多形式,但必须被全体参与的团体所知晓、接受。

② BP07.02。识别协调机制,有许多方法可以与其他工程组共享安全工程的决策和建议。本活动识别在项目中协调安全的不同方法。

③ BP07.03。促进协调,成功的关系依赖于良好的促进手段。在具有不同优先级(重要性)的不同机构之间进行沟通有可能会发生一些冲突。该基本实施确保争端以合适的、富有成果的方式得到解决。

④ BP07.04。协调安全决定和建议,该基本实施的目的在于在各种安全工程师、其他工程组、外部实体及其他可能的团体中沟通安全决策和建议。

3) PA08:监视安全态势

监视安全态势的目的在于确保标识并报告所有的可能导致安全问题的所有安全违规、试图的违规或错误。监视外部和内部环境可能对系统安全造成影响的所有因素。

(1) 基本实施列表。

① BP08.01。分析事件记录,以确定事件的原因、过程以及将来可能出现的事件。

② BP08.02。监视威胁、脆弱性、影响、风险和环境方面的变化。

③ BP08.03。识别与安全相关的突发事件。

④ BP08.04。监视安全措施的性能和功能的有效性。

⑤ BP08.05。检查系统的安全状态,确定有必要对系统实施的修改。

⑥ BP08.06。管理对相关安全相关事件的响应。

⑦ BP08.07。确保安全监视的结果得到适当保护。

(2)说明。

① BP08.01。分析事件记录,检测安全相关性信息的历史和事件记录(包括日志记录)。通过多条记录中的相关事件所用元素,应该能识别出感兴趣的事件。之后,多条事件记录可以融为一条事件记录。

② BP08.02。监视变化,查找可能影响当前安全态势有效性的任何变化,不管这种影响是正面的还是负面的。任何系统实施的安全应该与威胁、脆弱性、影响和风险相关联,因为它们与系统的内部和外部环境有关。这些因素没有一个是静态的,而变化既影响有效性,也影响适应性。必须监视所有因素的变化,并分析这些变化,以评估它们对安全有效性的影响。

③ BP08.03。识别安全突发事件,判断是否发生了安全事件,说明事件的详细情况,并在必要时做出报告。安全事件可利用历史事件的数据、系统配置数据、完整性工具和其他系统信息来检测。由于某些事件会经过一个较长周期时间后才出现,因此这种分析可能涉及与系统长时间状态进行比较。

④ BP08.04。监视安全防护措施,检测安全措施的性能,以标识出安全措施性能的变化。

⑤ BP08.05。检查安全态势。由于威胁环境、运行需求和系统配置等方面会出现变化,一个系统的安全态势可能会发生改变。本实施在于复查系统中实施安全的理由,并审查对其他工程领域或其他方面提出的安全需求。

⑥ BP08.06。管理安全突发事件响应，在许多情况中，系统的连续可用性是非常关键的。由于许多事件不能预防，因而对破坏的响应能力是至关重要的。应急计划要求标识出允许系统失效的最长时间；标识出系统中的重要功能组件；标识出并制订恢复战略和计划；测试这个计划并进行维护。在某些情况中，应急措施可能包括对突发事件的响应和与攻击者（例如病毒、黑客等）的对抗。

⑦ BP08.07。保护安全监视的记录数据，如果监视活动的成果不可信任，那么监视活动就没有价值。本实施包括对相关日志、审计报告和相关分析结果的封存与归档。

4）PA09：提供安全输入

提供安全输入的目的在于为系统的规划者、设计者、实施者或使用者提供他们所需的安全信息。这些信息包括安全体系结构、设计或实施的备选方案以及安全指南。同时与基于PA10“确定安全需求”中标识的安全需求，安全输入可以面向必要的机构成员而产生、分析和提供。此外，还应在这些成员间协调一致。

（1）基本实施列表。

① BP09.01。与设计者、开发者和用户合作，确保各方对安全输入需求达成共同的理解。

② BP09.02。判断在工程选择时所需的安全约束和安全考虑。

③ BP09.03。标识出与安全相关的工程问题备选解决方案。

④ BP09.04。利用安全约束和考虑因素对工程的备选方案进行分析并区分优先级。

⑤ BP09.05。向其他工程组提供安全相关的指南。

⑥ BP09.06。向运行系统的用户和管理员提供与安全相关的指南。

（2）说明。

① BP09.01。理解安全输入要求，安全工程与其他领域相协调，以判断这些领域所需的安全输入的类型。安全输入包括与安全相关的指南、设计、文档或思想。输入可以为多种形式，包括文档、备忘录、电子邮件、培训和咨询。这些输入基于PA10“确定安全需求”中的安全需求。例如，软件工程师就可能需要一套安全规则支持其工作。同系统相比，某些输入与环境的关联性更强。

② BP09.02。确定安全约束和考虑，该基本实施的目的在于为工程组确定所有的安全约束和考虑。安全工程组完成分析，从而为需求、设计、实现、配置和文档等确定所有的安全约束和考虑。安全约束可在系统生命期内的所有时间进行标识，并且可在许多不同的抽象层上进行标识。注意这些约束或是肯定的（总是如此）或是否定的（绝对禁止如此）。

③ BP09.03。标识安全备选方案，该基本实施的目的在于标识出与安全相关的工程问题的备选解决方案。这一过程要反复进行，将与安全相关的需求转化为具体的实现。这些解决办法可以多种形式提供，如体系结构、模型和原型。该基本实施涉及对安全相关需求的分解、分析和重组，直到确定有效的备选方案。

④ BP09.04。分析工程备选方案的安全性，该基本实施的目的在于分析和排列工程备选方案的优先级。使用BP09.02中确定的安全约束和考虑，安全工程师可以评估每个工程备选方案，并向安全工程组提交建议。此外，安全工程组还应考虑其他工程组的工程指南。这些工程备选方案不限于BP09.03所标识的安全备选方案，还可以包括来自其他领域的备选方案。

⑤ BP09.05。提供安全工程指南，该基本实施的目的在于制定安全相关的指南并把它提供给工程组。安全工程指南用于工程组对体系结构、设计和实现做出决策。

⑥ BP09.06。提供运行安全指南，该基本实施的目的在于，开发与安全相关的指南并提供给系统用户和管理员，告诉用户和管理员应以安全的方式进行安装、配置、运行和终止系统。为确保这一目的，运行安全指南的开发应在生命周期内提早开始。

5）PA10：确定安全需求

确定安全需求的目的在于明确标识出系统的安全相关需求。确定安全需求涉及为系统安全定义基本原则，以此满足有关安全的所有法律、策略、组织要求。安全需求应该基于系统的目标运行安全背景、当前的安全和机构的系统环境以及已标识的安全目标集来进行对照。

（1）基本实施列表。

① BP10.01。获得对客户安全需求的理解。

② BP10.02。标识出影响到系统的法律、政策、标准、外部影响和有关约束。

③ BP10.03。标识出系统的用途，以此来决定安全背景。

④ BP10.04。对系统运行形成一个高层的面向安全的认识。

⑤ BP10.05。形成高层目标，以定义系统安全。

⑥ BP10.06。为系统中实施的保护定义出一套一致的声明。

⑦ BP10.07。达成一致认识，使具体的安全需求能够满足客户的要求。

（2）说明。

① BP10.01。获得对客户安全需求的理解。该基本实施的目的在于收集所有有助于全面理解客户安全需求的信息。这些需求受到安全风险对客户重要性的影响。系统预期运行的目标环境也会影响客户与安全相关的需求。

② BP10.02。标识有关的法律、政策和约束。该基本实施的目的在于收集所有可能对系统安全产生影响的外部影响。可能的外部影响包括法律、法规、策略和商业标准。全局和局部政策的优先权应得到确定。必须说明系统客户提出的安全需求，并从中理解其安全意义。

③ BP10.03。识别系统安全背景。该基本实施的目的在于说明系统的背景是如何影响安全的。它涉及对系统（例如情报、金融、医疗）用途的理解。系统的任务处理和运行概要均要在安全考虑下加以评估。应对系统面临的威胁深入理解。评估性能和功能需求对安全可能产生的影响。运行的约束条件也要受到检查，以考察其对安全的影响。为定义系统的安全边界，环境可能也包括与其他机构或系统的接口。要标识接口组件位于安全边界的内侧或外侧。机构的许多外部因素也影响机构的安全需求。这些因素包括策略上的倾向性和政策重点的改变、技术发展、经济影响、全局性事件以及信息战。由于这些因素没有一个是静态的，因此需要监视和定期地评估这些变化可能造成的影响。

④ BP10.04。形成对系统运行的安全认识。该基本实施的目的在于形成一个高层的、面向安全的认识，包括角色、职责、信息流、资产、资源、人员保护以及物理保护，还要考虑在安全要求的约束下机构如何运作。这些应在运行安全概念中提出来，而且应该包括对系统体系结构、流程和环境的高层面的安全认识。与系统开发环境有关的要求也要在这一阶段进行收集。

⑤ BP10.05。形成安全的高层目标。该基本实施的目的在于标识出为了向运行环境

中的系统提供足够的安全而需满足的安全目标。PA06“建立保证论据”中确定的系统保证目标也会对安全目标产生影响。

⑥ BP10.06。定义安全相关需求。该基本实施的目的在于定义系统的安全相关需求。这一实施应确保每个需求与相关的政策、法律、标准、安全要求以及系统的约束条件协调一致。这些需求应完备地定义出系统的安全需求,包括那些通过非技术手段提供的需求。通常有必要定义或确定目标的逻辑或物理边界,以确保所有的方面都被提到。这些需求应与系统目标建立映射关系或发生关联。与安全相关的需求应被清楚地、简明地陈述,而且彼此不应发生矛盾。无论何时,安全都应将对系统功能和性能的任何影响降到最小。安全相关需求将为目标环境中的系统安全性提供评价的基础。

⑦ BP10.07。达成对安全的一致性认识。该基本实施的目的在于,使所有有关团体就安全需求达成一致性意见。当讨论普遍性用户时,安全需求要满足安全目标集。具体化的安全应能完备地、一致地反映有关的政策、法律和用户需求。在未达成一致性意见之前,应标识出相关问题,必要时可以返工。

3. 与保证过程相关的过程域

SSE-CMM 认为,保证是指安全需要得到满足的信任程度,SSE-CMM 的信任程度来自于安全工程过程可重复性的结果质量。与保证过程相关的过程如图 4-9 所示。

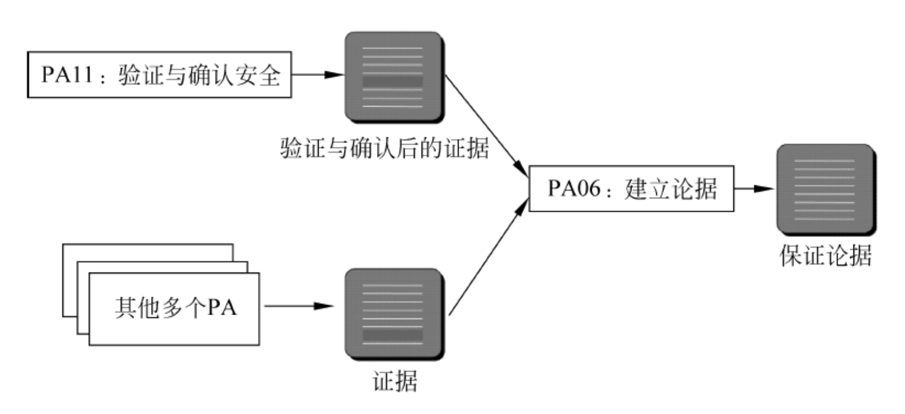


图 4-9 与保证过程相关的过程

1) PA11：验证与确认安全。

验证和确认安全的目的在于确保工程解决办法能够得到验证和确认。通过观察、示范、分析和测试,解决方案要在安全需求、体系结构和设计等方面得到检查。客户的运行安全验证将进一步对该方案提供确认。

(1) 基本实施列表。

① BP11.01。标识待验证和确认的解决方案。

② BP11.02。定义验证和确认的办法和严格程度。

③ BP11.03。验证解决方案是否实现了与上一抽象层相关的要求。

④ BP11.04。验证解决方案是否能最终满足客户的运行安全需求。

⑤ BP11.05。为其他工程组收集验证和确认的结果。

(2) 说明。

① BP11.01。标识验证和确认对象。该基本实施的目的在于分别标识出验证和确认

的对象。验证行为可证明解决方案已得到了正确的实施，而确认行为则证明了解决办法是有效的。它也涉及与整个生命周期内所有工程组的协调。

② BP11.02。定义验证和确认方法。该基本实施的目的在于定义验证和确认的方法和严格程度。标识过程涉及选择哪一种方法去对工程中每个需求实施验证和确认。严格程度可说明验证和确认的力度，这要受到 PA06“建立保证论据”中保证战略的影响。例如，某些项目只对需求的符合性进行简单的审查，而另一些则可能要求非常严格的检查。这一方法论还应包括维护可跟踪性的手段，跟踪的内容很多，从客户的运行安全需求到安全需要，到解决办法，再到验证和确认结果的方法。

③ BP11.03。实施验证。该基本实施的目的在于验证解决方案是否实现了上一抽象层相关的要求，包括 PA06“建立保证论据”中所标识的保证要求，从而验证解决方案是正确的。有许多验证需求的方法，包括测试、分析、观察和演示。所用的方法在 BP11.02 中标识。局部需求和整个系统的需求都要受到检测。

④ BP11.04。实施确认。该基本实施的目的在于验证解决办案能否最终满足客户的运行安全需求。有多种方法可以用来完成这项工作，包括在一个运行环境或有代表性的测试环境中去测试解决方案。所使用的方法应在 BP11.02 中被标识。

⑤ BP11.05。提供验证和确认的结果。该基本实施的目的在于为其他工程收集并提供验证和确认的结果。验证和确认的结果应以某种易被理解和使用的方式所提供。所有结果应被跟踪，以确保需求、解决办案以及测试结果的可跟踪性。

2）PA06：建立保证论据

建立保证论据的目的在于清楚地告诉客户，其安全需求已获满足。一个保证论据是一系列清晰陈述的保证目标。这些目标是由多个保证证据所支持，保证证据的来源和抽象级各不相同。

本过程包括标识和定义保证需求、证据的产生和分析活动、支持保证需求所需的附加证据。此外，对这些活动所生成的证据进行收集、整理并准备提交。

（1）基本实施列表。

① BP06.01。标识安全保证目标。

② BP06.02。定义面向所有保证目标的安全保证战略。

③ BP06.03。识别并控制安全保证证据。

④ BP06.04。对安全保证证据进行分析。

⑤ BP06.05。提供安全保证论据，以证明客户的安全需求得到满足。

（2）说明。

① BP06.01。标识安全保证目标，由客户确立的保证目标显示了用户对系统安全性的信任程度。系统安全保证目标规定了系统安全策略所提供的安全可信程度。该目标的充分性由开发者、集成者、客户和签字机关共同确定。对新增的安全保证目标或已有目标的修改均须得到确认，该工作要在工程机构内部和外部安全相关人员间得到协调（例如客户、系统安全认证机构、签字机关、用户等）。为反映变化，应不断更新安全保证目标。安全保证目标必须清晰地沟通，以确保没有异议。如有必要，应加入合适的解释。

② BP06.02。定义保证战略，安全保证战略的目的在于规划并确保安全目标能够正确地实现。安全保证战略在实施中所产生的证据应能（向系统的签字机关）提供一个可接受的

信心级,使其确信系统的安全措施足以管理安全风险。通过制定和实施安全保证战略,可实现对保证活动的有效管理。对保证需求的尽早标识和定义对于产生必要的支撑性证据是必要的。通过不断外部协调来理解和查看客户对保证需求的满意程度,这有助于确保得到高质量的保证需求包。

③ BP06.03。控制保证证据,安全保证证据要根据安全保证战略中的定义,通过与所有安全工程过程域相互配合,在不同抽象层面上标识出保证证据。这些证据要受到控制,以确保对当前的工作结果具有通用性,对安全保证目标具有关联性。

④ BP06.04。分析证据,引入保证证据分析,是为了保证所收集的证据能满足安全目标,从而满足顾客的安全需求。对保证证据的分析可说明系统安全工程和安全验证过程是否充分且足够,因而可以判断安全机制和安全特性是否令人满意地被实现。此外,对保证证据的分析,确保了工程实施结果相对于基线系统是完善和正确的。在保证证据不充分或不足够的情况下,本分析可能导致对支持安全目标的系统、安全工作结果和过程进行必要的修订。

⑤ BP06.05。提供保证论据,开发出一个全面的安全保证证据,以表明对安全保证目标的遵循性,并将保证证据提供给客户。保证论据是一系列已声明的保证目标的集合,由多层抽象度的保证证据所支持。为了满足安全目标,必须对提交证据中的缺陷和安全保证目标中的缺陷进行审查。

4.3.3 项目过程域和组织过程域

项目工程域包括5个过程:PA12,质量保证;PA13,配置管理;PA14,项目风险管理;PA15,技术成果的监控;PA16,技术成果的计划。在组织过程域中包括6个过程:PA18,提高组织系统工程过程;PA19,产品线进展管理;PA20,系统安全工程支持环境管理;PA21,提供在研的技术和知识;PA22,与供应商协调。

这两类过程域虽然并不直接同系统相关,但它们通过安全过程域的协调来保证安全工程的实施。

4.4 SSE-CMM能力级别

4.4.1 SSE-CMM能力级别简介

过程能力是由一组通用实施(GP)来衡量,通用实施是对所有工程过程都通用的工程实践。按照工程对于对通用实践的执行情况,可以将每个过程域按能力的高低分为6个级别,从第0~5级分别为未执行级、非正式执行级、计划和跟踪级、充分定义级、量化控制级及持续改进级。SSE-CMM的6个能力级别和公共特征,如图4-10所示。

1. 能力级别0:未执行级

0级能力水平指未执行能力级。未执行能力级的过程没有共同特征(CF)和通用实施(GP),在开发过程中没有安全工程思想的应用,但是当工程队伍中的关键人物不在或者当过程本身变得越来越复杂时,就难以保证任务的完成。

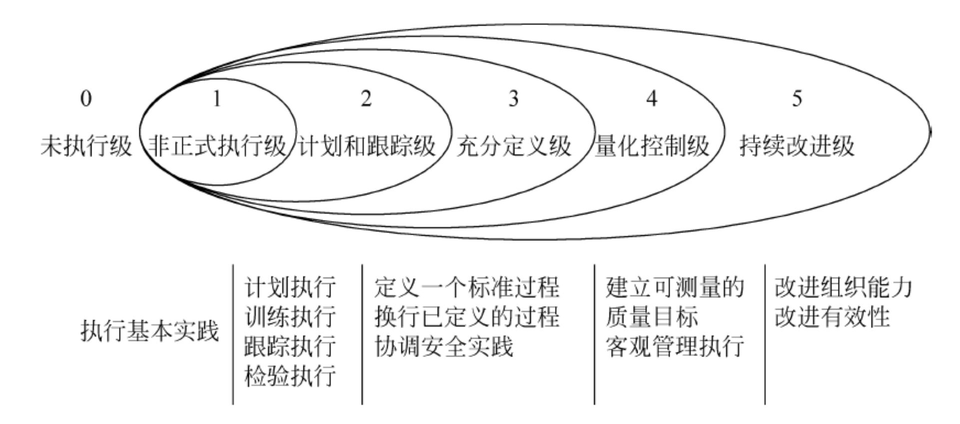


图 4-10　SSE-CMM 的 6 个能力级别和公共特征

2. 能力级别 1：非正式执行级

1 级能力水平指非正常执行的能力水平。所有的基本实施在一定程度上都能被执行，因而对过程能力缺少连续的计划和跟踪。产品质量和生产效率由工程队伍的所有人员的出色工作来保证。过程的执行还主要靠经验，对执行结果无明确要求，所以执行活动的能力是不可重复和被其他过程所借鉴的。

3. 能力级别 2：计划和跟踪级

2 级能力水平是指具有计划与跟踪的过程能力，它取决于安全工程基本实施的效率，因此与基本实施有关的工作过程可以被总结和控制。它与 1 级能力水平的不同之处在于此过程中的基本实施是可以重复和被其他组织借鉴的。

4. 能力级别 3：充分定义级

3 级能力水平是指完好定义的能力级水平。过程中的所有基本实施应按照完善定义的规范来进行，这些规范是工程队伍根据长期经验而总结出来的。它与 2 级能力水平的不同之处在于定义了一个被接受的标准规范，基本的实施可以反映出过程的特征，过程的能力可以直接转到其他工程活动中。

5. 能力级别 4：量化控制级

4 级能力水平是定量控制级水平。对每个已定义的过程和相联系的工作都设定出可度量的过程目标，可以对工程队伍和工程的进展进行定量的预测和控制。它与能力级别 3 的主要区别是所定义的过程是可量化理解和控制的。

6. 能力级别 5：持续改进级

5 级能力水平是持续完善的能力水平。从过程能力的角度看，它是最高水平，在此水平下已经建立了对过程效率的定性和定量的目标，而且可以准确地度量过程持续改善所获得的效益。它与能力级别 4 的主要区别是基于对这些过程变化效果的量化理解，工程中既定过程和标准过程将得到不断的改进和提高。

4.4.2　能力级别与通用实施的确定

能力级别反映一组共同特性，而每组共同特性可由通用实施来描述，具体关系如表 4-1 所示。

表 4-1 能力级别、公共特征及通用实施的关系

能力级别	公共特征	通用实施(GP)
0. 未执行	—	—
1. 非正式执行级	CF1.1 执行基本实施	GP1.1.1 执行过程
2. 计划和跟踪级	CF2.1 规划执行	GP2.1.1 分配资源
		GP2.1.2 分配责任
		GP2.1.3 文档化过程
		GP2.1.4 提供工具
		GP2.1.5 确保培训
		GP2.1.6 规划过程
	CF2.2 规范化执行	GP2.2.1 使用计划、标准和流程
		GP2.2.2 进行配置管理
	CF2.3 验证执行	GP2.3.1 验证过程遵循性
		GP2.3.2 审计工作结果
	CF2.4 跟踪执行	GP2.4.1 通过测量进行跟踪
		GP2.4.2 采取修正措施
3. 充分定义级	CF3.1 定义标准过程	GP3.1.1 对过程进行标准化
		GP3.1.2 裁减标准过程
	CF3.2 执行既定过程	GP3.2.1 使用充分定义的过程
		GP3.2.2 执行缺陷审查
		GP3.2.3 使用充分定义的数据
	CF3.3 协调安全实施	GP3.3.1 执行组内协调
		GP3.3.2 执行组间协调
		GP3.3.3 执行外部协调
4. 量化控制级	CF4.1 建立可测的质量目标	GP4.1.1 建立质量目标
	CF4.2 客观的管理过程的执行情况	GP4.2.1 确定过程能力
		GP4.2.2 使用过程能力
5. 持续改进级	CF5.1 改进机构的能力	GP5.1.1 建立过程的有效性目标
		GP5.1.2 持续改进标准过程
	CF5.2 改进过程的有效性	GP5.2.1 执行原因分析
		GP5.2.2 消除缺陷原因
		GP5.2.3 持续改进既定过程

4.5 小结

系统安全工程能力成熟度模型(SSE-CMM)是一种衡量安全工程实践能力的方法,是一种使用面向工程过程的方法。通过对安全工程过程的管理,将系统安全工程转变为一个完好定义的、成熟的、可测量的过程,具有此类成熟过程的组织开发的安全系统或产品具有较高安全确信度可重复性。SSE-CMM 模型的主要任务就是评测和改进整个信息安全系统整个生命周期当中的安全工程活动,到目前为止,这个模型是信息系统安全工程领域当中可靠性较高的针对性模型。

习　　题

1. SSE-CMM 工程过程包含哪些部分？它们之间如何协同工作？
2. ISSE 与 SSE-CMM 有什么不同？
3. 简单描述应用 SSE-CMM 确定组织的安全工程过程能力的步骤。
4. 使用 SSE-CMM 有什么好处？它适用于哪些场合？

第5章　信息安全风险管理与风险评估

本章学习目标：

- 了解风险管理的基本概念。
- 掌握信息安全风险评估方法。

5.1　信息安全风险管理

5.1.1　信息安全风险管理概述

风险管理最早起源于美国。由于受20世纪30年代世界性经济危机的影响，美国大量的银行和企业破产。为应对经营上的危机，许多大中型企业都在内部设立了保险管理部门，负责安排企业的各种保险项目。当时的风险管理主要依赖保险手段。1970年以后，随着企业面临的风险复杂多样和风险费用的增加，法国从美国引进了风险管理并在法国国内开始传播。同时，日本也开始了风险管理研究。风险在不同的领域有不同的定义及侧重点。本章主要介绍信息安全领域的风险及相应风险管理的内容。

风险(risk)，在信息安全领域是指信息资产遭受损坏并给企业带来负面影响的潜在可能性。

信息安全风险管理的概念因不同学者研究角度的不同而有不同的理解。如闵京华等认为“信息安全风险管理是基于风险的信息安全管理，也就是始终以风险为主线进行信息安全的管理”。

ISO 17799—2005定义信息安全风险管理为“指导和控制组织风险的协同活动，包括风险评估、风险应对、风险承受和风险沟通”。

NIST SP 800-30中定义信息安全风险管理为“对信息系统的风险识别、风险评估，并采取一定的措施使风险减少至可承受程度”。

Microsoft安全风险管理指南定义为“确定可接受的风险，评估风险的当前程度，采取措施将风险降低到可接受水平，以及维持风险程度的流程”。

Thomas Finne将其定义为“识别、评估和控制不确定性事件，并减少损失和提高安全投资收益，包括风险分析和风险评估”。

Mariana Gerber将其定义为“基于风险分析结果的风险计划、风险监控和风险控制”。

国际标准化组织制定的ISO/IEC 17799—2000中把信息安全风险管理定义为“以可接受的费用识别，控制、降低或消除安全风险的过程”。风险管理基本包含了通过风险评估来识别风险大小，通过制定信息安全策略，采取适当的控制目标与控制方式对风险进行控制，

使风险被避免、转移或降至一个可接受的水平。在风险管理方面应考虑控制费用与风险之间的平衡。

风险管理流程如图 5-1 所示。

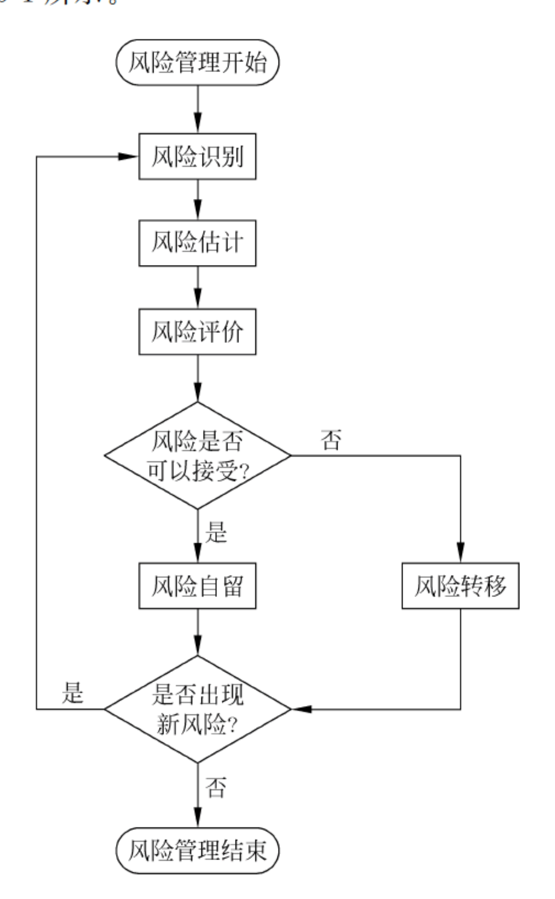


图 5-1　风险管理流程图

1. 信息安全风险管理的意义

在信息时代,信息是第一战略资源。一个机构需要利用其信息资产来完成使命,因此保障信息资产的安全至关重要。而资产与风险是天生的一对矛盾,资产价值越高,面临的风险就越大。信息资产有着与传统资产不同的特性,面临着新型风险。信息安全风险管理的目的就是要缓解和平衡这对矛盾,将风险控制在可接受的程度,保护信息及其相关资产,最终保证机构能够完成其使命。

信息安全风险管理贯穿信息系统生命周期的规划、设计、实施、运维和废弃各阶段中。每个阶段都存在着相关风险,同样需要采用信息安全风险管理的方法加以控制。

信息安全风险管理依据等级保护的思想和适度安全的原则,平衡成本与效益,合理部署和利用信息安全的信任体系、监控体系和应急处理等重要的基础设施,确定合适的安全措施,以保障机构完成其使命。

2. 信息安全风险管理的对象、角色与责任

信息安全风险管理涉及信息安全在信息、信息载体和信息环境 3 个方面中包含的所有相关对象。风险管理人员既包括风险管理的直接参与人员,也包括信息系统的相关人员。信息安全风险管理相关人员的角色与责任如表 5-1 所示。

表 5-1 信息安全风险管理相关人员的角色与责任

层面	信息系统			风险管理		
	角色	内外部	责任	角色	内外部	责任
决策层	主管者	内	负责信息系统的重大决策	主管者	内	负责风险管理的重大决策
管理层	管理者	内	负责信息系统的规划、建设、运行、维护和监控等	管理者	内	负责风险管理的规划,以及实施和监控过程中的协调
执行层	建设者	内或外	负责信息系统的设计和实施	执行者	内或外	负责风险管理的实施
	运行者	内	负责信息系统的日常运行和操作			
	维护者	内或外	负责信息系统的日常维护,包括维修或升级			
	监控者	内	负责信息系统的监视和控制	监控者	内	负责风险管理过程、成本和结果的监事和控制
支持层	专业者	外	为信息系统提供专业咨询、培训、诊断和工具等服务	专业者	外	为风险管理提供专业咨询、培训、诊断和工具等服务
用户层	使用者	内或外	利用信息系统完成自身的任务	受益者	内或外	反馈风险管理的效果

3. 风险管理的内容与过程

风险管理包括对象确立、风险分析、风险控制、审核批准、监控与审查、沟通与咨询 6 个方面的内容。

风险管理过程关系如图 5-2 所示。对象确立、风险分析、风险控制和审核批准是信息安全风险管理的 4 个基本步骤,监控与审查和沟通与咨询则贯穿于基本步骤中。

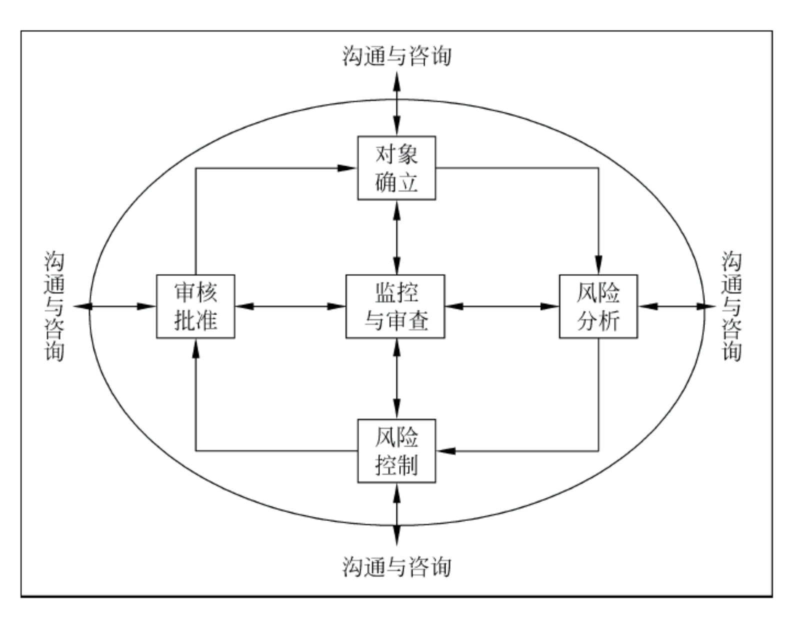


图 5-2 风险管理过程关系

5.1.2　生命周期各阶段的风险管理

信息安全风险管理、信息系统生命周期和信息安全目标均为正交关系，构成三维结构，如图 5-3 所示。

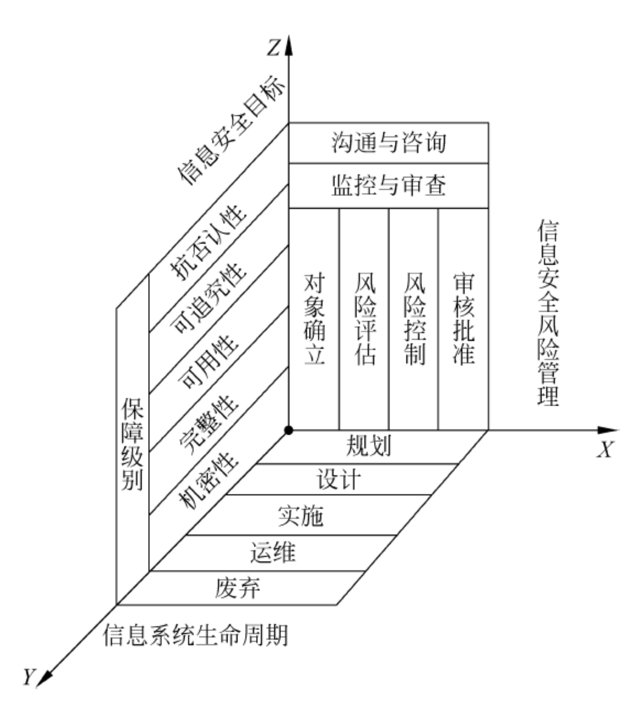


图 5-3　信息安全风险管理、信息系统生命周期和信息安全目标的三维结构关系

第一维（X 轴）：表示信息安全风险管理，包括对象确立、风险评估、风险控制和审核批准 4 个基本步骤，以及贯穿这 4 个基本步骤的监控与审查和沟通与咨询。

第二维（Y 轴）：表示信息系统生命周期，包括规划、设计、实施、运维和废弃 5 个基本阶段。

第三维（Z 轴）：表示信息安全目标，包括机密性、完整性、可用性、可追究性和抗否认性 5 个信息安全基本属性。

由图 5-3 可以看出，信息系统生命周期的任何一个阶段，都需要通过相应的信息安全风险管理，以实现安全目标，并最终完成信息系统等级化的保障体系建设。信息系统生命周期各阶段的特性、信息安全目标及信息系统保障级别随行业特点以及业务特性的不同而有所不同。

信息系统生命周期是某一信息系统从无到有，再到废弃的整个过程，包括规划、设计、实施、运维和废弃 5 个阶段。

1. 规划阶段的信息安全风险管理

在项目规划阶段，风险管理者应能清楚、准确地描述机构的安全总体方针、安全策略、风险管理范围、当前正在进行的或计划中将要执行的风险管理活动以及当前特殊安全要求等。为了保证项目规划阶段风险管理目标的实现，需要使用科学的风险管理方法。首先确定管理对象，然后通过恰当的风险分析方法来发现安全风险，对于这些风险采用适当的控制手段进行合理处理，以保证其达到机构核查批准的要求，使风险处于机构可接受的范围内。规划

阶段的风险管理活动如表 5-2 所示。

表 5-2 规划阶段的风险管理活动

序 号	风险管理活动	所处风险管理流程
1	明确安全总体方针	对象确立
2	安全需求分析	对象确立、风险分析
3	风险评价准则达成一致	风险控制、审核批准

由于上述风险管理活动处于项目的起始阶段，所以应特别重视沟通与监控环节。在项目的规划阶段，就安全目标、管理范围、评价准则等在机构内达成一致是项目顺利进行和成功完成的关键。

1）明确安全总体方针

机构管理安全总体方针制定过程中可能引入的安全风险，应先对安全总体方针文档的完整性、条理性、明确性等进行审查。审查的内容至少包括以下项目。

（1）是否已经制定并发布了能够反映机构安全管理意图的信息安全文件，如机构当前的业务期望、安全总体方针（包括定义边界关系、识别防御体系强度、识别各类主体）和安全策略等。

（2）风险管理过程的执行是否有机构保障，包括核查机构结构的合理性；核查职责分工的合理性，核查监控审查流程的合理性等。

（3）是否有专人按照特定的过程定期进行复审与评价，包括核查机构当前的风险管理复查流程；核查复查情况及调整计划；核查能否确保当系统安全状态发生变化时及时进入复审与评价的过程，以便及时地修改安全策略，恢复到机构可接受的安全状态等。

（4）风险管理的范围是否明确。

以上项目需根据机构的具体情况进行增加或删减，但至少应建立符合机构业务战略的安全总体方针，从而使机构安全风险管理有助于业务的运行。对于安全总体方针的核查流程须得到相关部门的审核批准。

2）安全需求分析

机构可通过以下方法来管理安全需求分析过程中可能引入的安全风险：应对安全需求分析文档的完整性、条理性、明确性等进行审查；应采用信息安全风险分析方法，通过对信息系统进行风险评估来发现当前安全保障体系中存在的不足。

对于安全需求分析文档的核查流程须得到机构相关部门的审核批准。

3）风险评价准则达成一致

机构可通过以下方法来管理风险评价准则制定过程中可能引入的安全风险。

（1）机构应对文档的完整性、条理性、明确性等进行审查。

（2）机构可通过问卷调查或专人访谈的方式核查评价准则是否得到机构一致性的认可。核查项目包括风险管理的要素和风险评价准则是否得到一致性认可。

对于风险评价准则，机构应保证准则文档的清晰性和明确性，以及是否得到机构的一致性认可。如果风险评价准则不能达成一致，这将直接导致无法对风险做出公认的评价，从而导致风险评估的失败。

2. 设计阶段的信息安全风险管理

设计阶段是依据项目规划阶段输出的总体方案来设计信息系统的实现结构(包括功能划分、接口协议和性能指标等)和实施方案(包括实现技术、设备选型和系统集成等)。在设计信息系统的实现结构和实施方案时,在技术的选择、配合、管理等众多的环节均容易引入安全风险,因此对关键的环节应提出必要的安全要求并有针对性地进行安全风险管理。

在该阶段的主要安全需求包括:对用于实现安全系统的各类技术进行有效性评估;对用于实施方案的产品须满足安全保护等级的要求;对自开发的软件要在设计阶段就充分考虑安全风险。

在设计阶段,风险管理者应能标识出在项目结构实现过程中潜在的安全风险,为设计说明中的安全性设计提供评判依据,并对实施方案中选择的产品进行合格检查,确保项目设计阶段的重要环节均能得到较好的安全风险控制。

在该阶段的风险管理工作过程中,主要面临设计阶段的风险管理活动(如表 5-3 所示)。

表 5-3　设计阶段的风险管理活动

序　号	风险管理活动	所处风险管理流程
1	安全技术选择	风险控制
2	安全产品选择	风险控制
3	软件设计风险控制	风险控制

对于上述风险管理活动,机构应该注重通过足够的外部咨询来学习、了解各种技术和产品的优缺点,并在充分的内部沟通的基础上得出技术选择说明、产品选型说明以及软件安全要求文档。

1) 安全技术选择

机构可通过如下方法来管理安全技术选择过程中可能引入的安全风险,从而构建符合要求的安全保障体系,包括参考现有国内外安全标准、国内外公认安全事件、行业标准,专家委员会决策。

在项目设计阶段,需充分考虑所选择的安全技术能够解决问题的程度,即技术选择的有效性。如果技术选择不合理,将直接导致相应安全弱点的暴露,安全风险的发生将是显而易见的。

对于技术选择文档的核查流程须得到机构相关部门的审核批准。

2) 安全产品选型

机构可通过如下方法来管理安全产品选型过程中可能引入的安全风险,包括核查是否符合相关安全标准要求、是否通过相关认证机构的认证,是否满足当前安全保障等级的要求;核查产品的实用性;集中测试;专家会议决策。

安全产品选型的合理程度将直接影响原有设计方案所需要达到的安全防御效果,因此在项目设计阶段要做好安全产品选型工作。

对于产品选型文档的核查流程须得到机构相关部门的审核批准。

3) 软件设计风险控制

机构可通过如下方法来管理自开发的非通用软件在前期设计过程中可能引入的安全风险,包括清晰描述软件的安全功能需求,在设计规格说明书中明确指出实现的方法,参考

GB/T 18336.1-2015 对设计说明书的安全功能进行核查、补充、完善,以及对各安全功能进行详细的功能测试。

对于自主开发的非通用软件,通常由于各种原因而存在众多的安全风险,这些风险直接影响了系统的正常运行。另外,在软件设计阶段就考虑好如何规避安全风险,这样做比实现之后再进行补救节省大量的成本。因此,在设计阶段对软件进行风险控制是非常必要和有意义的。对于软件设计说明文档的核查流程须得到相关部门的审核批准。

3. 实施阶段的信息安全风险管理

实施阶段将按照规划和设计阶段所定义的信息系统实施方案,采购设备和软件,开发定制功能,集成、部署/配置和测试系统,并对是否允许系统投入运行进行审核批准。

实施阶段的安全需求包括:确保采购的设备、软件和其他系统组件满足已定义的安全要求;确保定制开发的软件和系统满足已定义的安全要求;确保整个系统已按照设计要求进行部署和配置,并通过整体的安全测试来验证系统的安全功能和安全特性是否符合设计要求;通过对相关人员的操作培训和安全培训,确保人员已具备维持系统安全功能和安全特性的能力;通过对系统投入运行前的审核批准,确保信息系统的使用已得到授权。

在实施阶段,风险管理的主要目标是确保上述安全需求已得到实现。

实施阶段的风险管理活动主要包括检查与配置、安全测试、人员培训及授权系统运行,同时在上述过程中通过监控与审查、沟通与咨询来确保本阶段风险管理目标的实现。各项活动在风险管理流程中所处的位置如表 5-4 所示。

表 5-4 实施阶段的风险管理活动

序 号	风险管理活动	所处风险管理流程
1	检查与配置	风险控制
2	安全测试	风险控制
3	人员培训	风险控制
4	授权系统运行	审核批准

在系统安全功能和安全特性、测试计划和测试过程方面进行充分沟通,并相互配合来完成风险控制的工作。信息系统安全员还应监控上述实施过程,如发现问题应及时向主管领导汇报。

1) 检查与配置

应对采购的设备、软件、定制开发的软件和系统进行检查并正确配置。检查与配置内容包括:检查采购的设备和软件是否具有国家主管部门的生产和销售许可证,以及是否通过了国家有关部门的测评和认证;检查采购的设备、软件和系统是否具备安全功能和安全特性;按照产品说明书和设计说明书正确配置设备、软件和系统,确保符合设计要求。

如果在系统实施的过程中增加了新的安全控制措施,还应对新增加的措施给原有系统带来的风险进行分析,确保增加的控制措施与原有设计保持协调一致。

2) 安全测试

系统安全测试是对所开发或采购的系统特定部分的测试和整个系统的测试。测试内容包括:采购的设备和软件、定制的软件和系统各部分安全功能及安全特性的测试;对集成后整个系统的整体安全测试;对安全管理、物理设施、人员、流程、业务或内部服务(如网络

服务)的使用,以及应急计划等进行测试。

如果在开发或采购阶段增加了新的控制措施,应重新进行测试。安全测试可以由机构内部实施,也可以聘请第三方专业机构实施。

测试之前应制订测试计划,并对测试过程和测试结果进行记录。

3) 人员培训

培训的对象包括系统使用人员、系统维护人员和安全管理人员,培训过程是沟通与咨询的重要体现。培训内容包括:系统的操作流程和操作方法,安全意识、基本安全技术知识和安全管理知识,系统维护和安全功能的使用,安全管理制度的管理流程,系统安全事件的应急处理流程和恢复流程。

4) 授权系统运行

信息系统在投入运行前应进行审核批准。负责审批的管理者应与系统安全员、系统管理人员、系统使用人员进行充分沟通,必要时还可以聘请专家进行咨询,以便对系统是否可以投入运行做出重要决策。管理者对信息系统可以有以下 3 种授权方式。

(1) 授权系统全面运行。即在对安全测试的结果进行评估之后,如果系统的参与风险被认为是完全可以接受的,那么就可以为系统发布一个全面运行的授权。这时信息系统已被认可,可以没有限制或没有制约地投入运行。

(2) 临时批准运行。即在对安全测试的结果进行评估之后,如果系统的参与风险被认为不能完全接受,但是又迫切需要将信息系统投入运行,或机构的使命需要其继续运行,那么就会为信息系统发布一个临时的运行批准。临时批准提供的是一种有限制的授权,允许信息系统在特定时限和条件下投入运行,并使相关人员了解到机构的运行和资产在限定时间内具有相对更高的风险。临时运行额定允许时限应与信息系统的风险等级相关联,最长不应超过一年。在临时批准运行结束前,信息系统应满足全面批准运行的条件,开始全面批准的运行,否则应停止系统运行。

(3) 拒绝对运行进行授权。即在对安全测试的结果做出评估之后,如果系统的残余风险被认为是不可接受的,那么就要拒绝批准信息系统投入运行。对于被拒绝运行的系统,信息系统所有者应与授权管理者和其他相关方进行沟通,重新制订风险控制措施和改进计划,将信息系统的安全风险降低到可接受的程度后,再进行授权审批。

4. 运维阶段的信息安全风险管理

运维阶段是在信息系统经过授权投入运行之后,通过风险管理的相关过程和活动,确保信息系统在运行过程中以及信息系统或其运行环境发生变化时维持系统的正常运行和安全性。

运维阶段的安全需求包括以下内容:在信息系统未发生更改的情况下,维持系统的正常运行,进行日常的安全操作及安全管理;在信息系统及其运行环境发生变化的情况下,进行风险评估并针对风险制定控制措施;定期进行风险再评估工作,维持系统的持续安全;定期进行信息系统的重新审批工作,确保系统授权时间的有效性。

在运维阶段,风险管理的主要目标是确保上述安全需求得到实现。

运维阶段的风险管理活动主要包括安全运行和管理、变更管理、风险再评估、定期重新审批,同时在上述过程中通过监控与审查、沟通与咨询来确保本阶段风险管理目标的实现。各项活动在风险管理流程中所处位置如表 5-5 所示。

表 5-5　运维阶段的风险管理活动

序　号	风险管理活动	所处风险管理流程
1	安全运行和管理	风险控制
2	变更管理	风险评估、风险控制
3	风险再评估	风险评估、风险控制
4	定期重新审批	审核批准

安全运行和管理活动贯穿于整个运维阶段，在系统发生变化、运行环境发生变化，以及发现新的脆弱性的情况下，应进行系统变更管理，并将管理要求反馈到安全运行与管理活动中；在变化较大的情况下，应进行风险再评估，再评估活动也应定期进行；系统授权运行的重新审批工作也应定期进行，以保证系统授权时间的有效性。

运维阶段风险管理活动流程如图 5-4 所示。

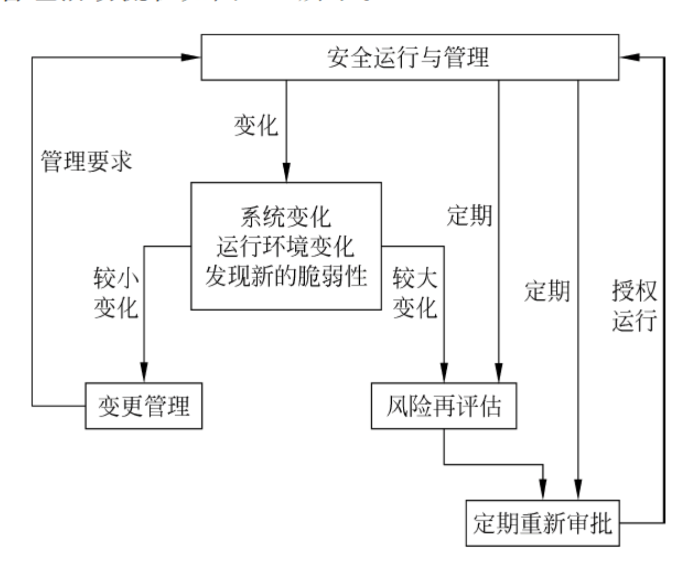


图 5-4　运维阶段风险管理活动流程

1）安全运行和管理

信息系统在开始运行之后，应按照控制措施所定义的系统操作要求、运行要求和管理要求，进行安全操作和安全管理，保证系统的安全功能的实现。安全运行和管理包括执行备份、举办培训课程、管理密钥、更新用户管理和访问特权以及更新安全软件等。

2）变更管理

在信息系统及其与运行环境发生变化时，应评估其风险，并制定和实施相应的控制措施以控制风险。变更管理包括信息系统的变更和系统运行环境的变更；信息系统的变更包括系统升级、增加新功能、发现新的系统威胁和脆弱性等；系统运行环境的变更包括系统的硬环境、软环境的变化，以及法律法规环境的变化。

在信息系统及其运行环境发生变化时，应执行风险管理流程中的风险评估过程和风险控制过程，分析可能出现的新风险，并制定和实施控制措施对风险进行控制。

变更管理主要用于信息系统及其运行环境变化不大的情况，变更管理无须对系统运行进行重新授权。

3）风险再评估

风险再评估是重新对系统进行风险评估的过程。应定期进行系统的风险再评估，在信息系统及其运行环境发生重大变化时，也应适时进行风险再评估。定期风险评估的周期一般应为一年，最长不应超过两年。

风险再评估后应执行风险控制过程，针对风险制定和实施控制措施。

4）定期重新审批

定期重新审批是重新执行信息系统审核批准的过程。信息系统在运行一段时间之后，系统及其运行环境、风险环境都会发生变化，应重新确认系统风险是否仍在可接受的范围内。

信息系统授权的重新审批应以风险再评估的结果为依据，根据系统风险再评估后的风险状况和残余风险，重新审批信息系统是否可以继续运行。

5. 废弃阶段的信息安全风险管理

废弃阶段是对信息系统的过时或无用部分进行报废处理的过程。在废弃阶段，风险管理的目标是确保信息、硬件、软件在执行废弃的过程中的安全废弃，防止信息系统的安全目标遭到破坏。

在这一阶段主要的风险管理活动是对系统报废的风险评估和风险控制。

系统废弃阶段涉及信息、硬件和软件的安全处置，应防止敏感信息被泄露给外部人员。系统废弃的风险管理活动包括：确定废弃对象，对废弃对象的风险分析，对废弃对象及废弃过程的风险控制。同时在上述过程中通过监控与审查、沟通与咨询来确保本阶段风险管理标的实现。各项活动在风险管理流程中所处位置如表 5-6 所示。

表 5-6　废弃阶段的风险管理活动

序　号	风险管理活动	所处风险管理流程
1	确定废弃对象	对象建立
2	废弃对象的风险分析	风险分析
3	废弃过程的风险控制	风险控制
4	废弃后的评审	审核批准

1）确定废弃对象

信息系统在经过一段时间的运行及使用之后，系统的部分或全部可能不再需要。这时要对需要废弃的部分进行分析，确定系统的哪些部分需要废弃。废弃对象的考虑范围包括被废弃的信息、硬件、软件或整个系统。应建立废弃对象的清单，并进行标识。

2）废弃对象的风险分析

废弃系统的风险分析主要应考虑被废弃的信息、硬件和软件的安全要求，分析废弃对原有系统造成的威胁和脆弱性，评估不安全废弃可能带来的影响和可能性。

3）废弃过程的风险控制

废弃过程的风险控制应考虑建立废弃系统的安全处置程序，可考虑以下控制措施：对载有敏感信息的介质应加以安全、妥当的保存或采用安全的方式加以处置，如焚烧或碎片，或在清空数据后供本机构内的其他方面使用；把所有的媒体收集起来并进行安全的处置，比试图分离出敏感的物品可能更加容易；许多机构对文件、设备和媒体提供收集和处置的

服务。应注意选择一个具有足够的控制措施和有经验的承包商；若可能，对敏感物品的处置应进行记录。

在等候集中处理时，应当考虑聚集效应，即大量未分类信息堆积在一起可能比少量已分类的信息更敏感。

4）废弃后的评审

在执行完废弃过程后应对系统废弃后的残余风险进行评审，以确保参与风险是在用户可接受的范围内。评审的内容包括确认废弃后系统中的敏感信息已被有效清除，系统废弃的安全要求已得到满足。

5.2 信息安全风险评估

5.2.1 风险评估概述

1. 风险评估的基本概念及作用

信息安全风险评估指的是依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

风险评估的主要任务包括：识别组织面临的各种风险，评估风险概率和可能带来的负面影响，确定组织承受风险的能力，确定风险消减和控制的优先等级，推荐风险消减对策。

风险评估的操作范围可以是整个组织，也可以是组织中的某一部门，或者独立的信息系统、特定系统组件和服务。影响风险评估进展的因素包括评估时间、力度、展开幅度和深度，它们都应与组织的环境和安全要求相符合。组织应该针对不同的情况来选择恰当的风险评估途径。按照信息系统风险评估的范围及对象，实际工作中信息系统风险评估可以包括综合评估、详细评估和态势评估等。

通过信息安全风险评估，能够清晰地了解当前所面临的安全风险与信息系统的安全现状；明确地看到当前安全现状与安全目标之间的差距；为下一步控制和降低安全风险、改善安全状况提供客观和翔实的依据。

信息安全风险评估的工作形式一般包括自评估和检查评估两种形式。其中，自评估适用于对自身信息系统进行安全风险的识别、评价。自评估可以委托风险评估服务技术支持方实施，也可以自行实施。检查评估一般由主管机关发起，通常都是定期的、抽样进行的评估模式，旨在检查关键领域或关键点的信息安全风险是否在可接受的范围内。风险评估应以自评估为主，检查评估在自评估过程记录与评估结果的基础上，验证和确认系统存在的技术、管理和运行风险，以及用户实施自评估后采取风险控制措施所取得的效果。

2. 信息系统安全风险评估模型

信息系统的安全风险可分解成资产的影响、威胁的频度和脆弱性的严重程度三要素，其模型如图 5-5 所示。

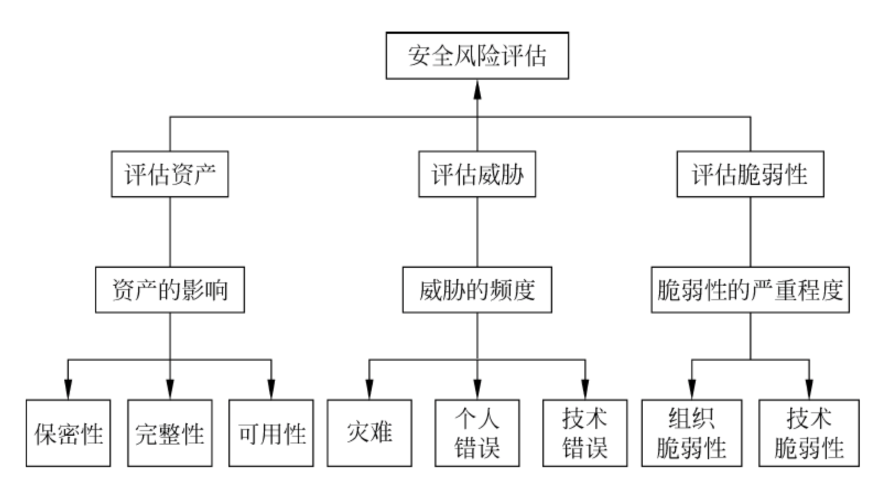


图 5-5　信息系统安全风险评估模型

5.2.2　风险评估策略

1. 风险评估原则

风险评估一般应遵循以下几个原则。

1）标准性原则

风险评估方案的设计应遵循国家政策法规、技术规范与管理要求、行业标准和国际标准。风险评估的具体实施流程应该由专业的风险评估人员依据评估与被评估方共同设计的标准流程进行。

2）可控性原则

可控性包括人员可控性、工具可控性和项目可控性。所有参与风险评估工作的人员均应进行严格的资格审查和备案，明确其职责，需要进行人员调整或者工作岗位变更时，必须执行严格的审批手续。

3）完整性原则

严格按照委托单位的评估要求和指定的范围进行全面的评估服务，避免由于遗漏造成的不全面风险评估。

4）最小影响原则

风险评估工作可能会导致信息系统的性能明显下降、网络阻塞、服务中断等，还可能会影响业务的正常运行，因此，在风险评估过程中，应该从项目管理层和工具技术层出发，将风险评估对信息系统正常运行造成的影响降到最小。

5）保密原则

风险评估双方签署保密协议和非侵害协议，评估过程中所获知的被评估系统的任何信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何被评估组织的网络和信息系统的行为。

2. 风险评估的基本特点

风险评估具有以下基本特点。

1）决策支持性

所有的安全风险评估都旨在为安全管理提供支持和服务，无论它发生在系统生命周期

的哪个阶段，所不同的只在于其支持的管理决策阶段和内容。

2）比较分析性

对信息安全管理和运营的各种安全方案进行比较，对各种情况下的技术、经济投入和结果进行分析、权衡。

3）前提假设性

在风险评估中所使用的各种评估数据有两种：一种是系统既定事实的描述数据；另一种是根据系统的各种假设前提条件确定的预测数据。不管发生在系统生命周期的哪个阶段，在评估时，人们都必须对尚未确定的各种情况做出必要的假设，然后确定相应的预测数据，并据此做出系统风险评估。没有哪个风险评估不需要给定假设前提条件，因此信息安全风险评估具有前提假设性这一基本特性。

4）时效性

必须及时使用信息安全风险评估的结果，加强信息安全管理，增强信息安全有效防护。

5）主观与客观集成性

信息安全风险评估是主观假设和判断与客观情况和数据的结合。

6）目的性

信息安全风险评估的最终目的是为信息安全管理决策和控制措施的实施提供支持。

信息安全风险评估的这些基本特点将在很大程度上影响风险评估的操作方式和操作结果。

5.2.3 风险评估方法

在进行信息安全风险评估之前，收集必要的信息数据可以掌握信息的安全现状，同时也是后续工作的前提条件。根据信息的获取手段和方式可以分为以下 5 种。

(1) 直接获取。

(2) 设计不同的调查问卷。例如，对组织的信息安全管理人员设计组织的管理类控制调查表；对系统管理员设计本系统的运行类控制调查表；对资产的具体负责人设计资产的运行情况调查表。

(3) 现场面谈与参观。

(4) 文档检查。策略文档、系统文档、安全相关的文档可以提供关于待评估系统已经使用或计划使用的安全控制方面的有用信息。

(5) 使用自动扫描工具。一些主动的技术方法可以被用作有效的收集系统信息，如可以检查系统存在的漏洞、口令强度、访问权限控制、用户账号限制、数据完整性和机密强度等安全信息。

1. 定量评估方法

定量评估方法是指运用数量指标对风险进行评估。采用量化的数值描述后果和可能性。定量评估方法以获取到或采取一定方法量化后得到的被调查对象的定量数据为基本材料，依据一定的算法进行分析、计算、综合，然后得出结果数据。

定量评估方法一般适用于确立威胁发生概率、预测系统风险发生概率、确立系统总体风险评价等。例如，对运行在某个平台上的不同主机、应用系统分别进行等价化的赋值，综合分析每个资产的威胁、脆弱性，得到各资产的风险量化值。典型定量风险评估方法有因子分

析法、聚类分析法、时序模型、回归模型、风险图法和决策树法等。

定量评估方法的优点是用直观的数据来表述评估的结果，看起来一目了然，而且比较客观。定量评估方法的采用，可以使研究结果更科学、更严密、更深刻。

定量评估是定性评估的基础和前提，定性评估应该建立在定量评估基础之上。

2. 定性评估方法

定性评估方法主要依据研究者的知识、经验、历史教训、政策走向等非量化资料对系统风险状况做出判断的过程。采用文字形式或叙述性数值范围描述风险的影响程度和可能性的大小，如高、中、低等。定性评估方法一般适用于风险识别、造成风险的原因分析、威胁发生所造成的影响分析等。例如针对操作系统、采用扫描工具、发现其漏洞并指明漏洞的严重程度。

定性评估方法有过程危害分析、检查表分析、失误模式与影响分析、故障树分析、危害与可操作性分析。

定性评估方法避免了定量方法的缺点，可以挖掘出一些蕴藏很深的思想，使评估的结论更全面、更深刻；但它的主观性很强，对评估者本身的要求很高。

定性分析是灵魂，是形成概念、观点，做出判断，得出结论所必须依靠的。

3. 定性与定量相结合的综合评估方法

系统风险评估是一个复杂的过程，需要考虑的因素很多，有些评估要素可以用量化的形式来表达，而对有些要素的量化又是很困难甚至是不可能的，所以不主张在风险评估过程中一味地追求量化，也不认为一切都是量化的风险评估过程是科学、准确的。定量分析是定性分析的基础和前提，定性分析应建立在定量分析的基础上才能揭示客观事物的内在规律。在复杂的信息系统风险评估过程中，不能将定性分析和定量分析两种方法简单地割裂开来，而是应该将这两种方法融合起来，采用综合的评估方法。

定量评估方法和定性评估方法的优缺点对比如表 5-7 所示。

表 5-7　定量评估方法和定性评估方法的优缺点对比

分析方法	定量评估方法	定性评估方法
优点	评估结果是建立在独立客观的程序或量化指标之上的	计算方式简单，易于理解和执行
	量化的资产价值和预期损失易理解	不必精确算出资产价值和威胁频率
	可利用自动化工具帮助分析	流程和报告形式比较有弹性
	可以为成本效益审核提供精确依据	不必精确算出推荐的安全措施的成本
缺点	没有一种标准化的知识库，依赖于提供工具或实施调查的厂商	本质上是主观的，结果高度依赖于评估者的经验和能力，很难客观地跟踪风险管理的效果
	信息量大，计算量大，方法复杂	对关键资产财务价值评估参考性较低
	投入大，费时费力	并不能为安全措施的成本效益分析提供客观依据

在复杂的信息系统风险评估中，不能将定性分析与定量分析简单地分割开来。评估过程中对于结构化很强的问题，采用定量评估方法；对于非结构化的问题，采用定性评估方

法，对于兼有结构化特点和非结构化特点的问题，采用定性与定量相结合的评估方法。3种综合风险评估方法的比较如表5-8所示。

表5-8 3种综合风险评估方法的比较

评估方法	特点	优点	缺点
概率风险评估	以定性评估和定量计算相结合，将系统逐步分解转化为初始事件，进行分析确定系统失效的事件组合及失效概率	识别风险及原因，给出导致风险的事故序列和事故发生的概率	要求数据收集的准确性和全面性
动态概率风险评估	能够与时间紧密结合，确定系统失效的事件组合及失效概率	识别风险及原因，给出导致的事故序列和事故发生的概率，而且具备动态性	要求数据收集的准确性和全面性，且时间要求较紧
层次分析法	对系统进行分层次、拟定量、规范化处理，为决策者提供定量形式的决策依据	对决策分析问题的解决提供了好方法，可以评估最底层各个元素在总目标中的风险程度	需要求解判断矩阵的最大特征根及其对应的特征向量

5.2.4 风险评估实施流程

风险评估实施流程包括评估准备，对资产、威胁、脆弱性的识别，对已采取的安全措施的确认以及风险识别等环节。风险评估实施流程图如图5-6所示。

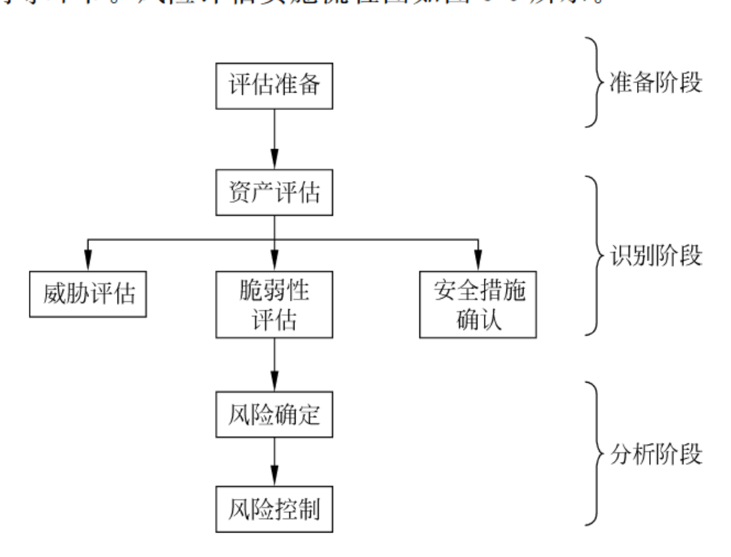


图5-6 风险评估实施流程

1. 风险评估的准备

风险评估的准备是整个风险评估过程有效性的保证。组织实施风险评估是一种战略性的考虑，其结果将受到组织业务战略、业务流程、安全需求、系统规模和结构等方面的影响。因此，在风险评估实施前，应该做如下风险评估的准备。

(1) 确定风险评估的目标。风险评估的准备阶段应明确风险评估的目标，为风险评估的过程提供导向。风险评估的目标是满足组织业务持续发展在安全方面的需求，或符合相关方的要求，或遵守法律法规的规定等。

(2) 确定风险评估的范围。基于风险评估目标确定风险评估范围是完成风险评估的前提。

(3) 组建适当的评估管理与实施团队，以支持整个过程的推进。

(4) 选择与组织相适应的具体的风险判断方法。应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险判断方法，使之能够与组织环境和安全要求相适应。

(5) 获得最高管理者对风险评估工作的支持。

风险评估准备阶段对输出文档的要求如表5-9所示。

表5-9　风险评估准备阶段对输出文档的要求

阶　段	输出文档	文档内容
风险评估准备	《风险评估计划书》	风险评估的目的、意义、范围、目标、组织结构、经费预算和进度安排等
	《风险评估程序》	风险评估的工作流程、输入数据和输出结果等
	《入选风险评估方法和工具列表》	合适的风险评估方法和工具类别

2. 资产识别和威胁识别

1) 资产识别

(1) 资产定义。资产是被机构直接赋予了价值因而需要保护的东西。资产可能以多种形式存在，如无形的与有形的，硬件与软件，文档与代码等。

(2) 资产分类。资产有多种表现形式，同样的两个资产也因属于不同的信息系统而重要性有所不同。首先需要将信息系统及相关的资产进行恰当的分类，以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者灵活把握。

根据资产的表现形式，资产分为数据、软件、硬件、文档、服务、人员等类型。

(3) 资产赋值。根据资产的重要程度可以进行等级化处理，不同的等级分别代表资产重要程度的高低。等级数值越大，重要程度越高。

在对信息系统进行安全风险评估中，对资产的赋值不仅要考虑资产的经济价值，更要考虑资产的安全状况，即资产的机密性、完整性及可用性对组织信息安全性的影响程度。资产重要度赋值表如表5-10所示。

表5-10　资产重要度赋值表

赋　值	标　识	定　义
5	很高	资产的重要程度很高，其安全属性被破坏后可能导致系统受到非常严重的影响
4	高	资产的重要程度较高，其安全属性被破坏后可能导致系统受到比较严重的影响
3	中等	资产的重要程度较高，其安全属性被破坏后可能导致系统受到中等程度的影响
2	低	资产的重要程度较低，其安全属性被破坏后可能导致系统受到较低程度的影响
1	很低 (可忽略)	资产的重要程度很低，其安全属性被破坏后可能导致系统受到很低程度的影响，甚至忽略不计

2）威胁的频度

（1）威胁定义。威胁是一种对组织及其资产构成潜在破坏的可能性因素，是客观存在的。一项资产可能面临着多个威胁，同样一个威胁可能对不同的资产造成影响。

（2）威胁分类。产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素又可以分为有意和无意两种；环境因素包含自然界的不可抗的因素和其他物理因素。

对威胁进行分类的方式多种多样，根据造成威胁的原因可以把威胁分为软硬件故障、物理环境威胁、操作失误、管理不到位、恶意代码和病毒、越权或滥用、网络攻击、泄密、篡改、抵赖等。

（3）威胁赋值。判断威胁出现的频率是威胁识别的重要工作，评估者应根据经验和有关的统计数据来进行判断。

可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现频率的高低，等级数值越大，威胁出现的频率越高。

威胁频率赋值表如表 5-11 所示。

表 5-11　威胁频率赋值表

赋　值	标　识	定　义
5	很高	出现的频率很高(或大于 1 次/周)，或在大多数情况下几乎不可避免，或可以证实经常发生过
4	高	出现的频率较高(或次/月)，或在大多数情况下很有可能会发生，或可以证实多次发生过
3	中	出现的频率中等(或大于 1 次/半年)，或在某种情况下可能会发生或被证实曾经发生过
2	低	出现的频率较小，或一般不太可能发生，或没有被证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见和特殊的情况下发生

3. 脆弱性识别

1）脆弱性定义

脆弱性(vulnerability)：可能会被一个或者多个威胁所利用的资产或一组资产的弱点(weakness)。弱点是资产本身存在的，它可以被威胁利用，引起资产的损害。弱点包括物理环境、机构、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。

从定义可以看出，首先，脆弱性是“资产或者一组资产”的弱点。弱点都是相对而言的。其次，“可能会被一个或者多个威胁所利用”的弱点才能称为脆弱性。也就是说，之所以能成为脆弱性，是因为这个弱点可能会被外界威胁利用而造成实际的影响，如果这个弱点找不到可以利用它的威胁，那么，这仅仅是弱点，而不是脆弱性。

弱点虽然是资产本身固有的，但它本身不会造成损失，它只是一种可能被威胁利用而造成损失的条件或环境。所以，如果没有相应的威胁发生，单纯的弱点并不会对资产造成损害。那些暂时没有安全威胁的弱点可以不需要实施安全保护措施，但必须被记录下来，以确保当环境、条件有所变化时能随之加以控制。需要强调的是，不正确的、起不到应有作用的或没有正确实施的安全保护措施本身就可能是一个安全薄弱环节。

脆弱性识别所采用的方法主要有问卷调查、人员问询、工具扫描、手动检查、文档审查、

渗透测试等。脆弱性识别将针对每一项需要保护的信息资产，找出每一种威胁所能利用的脆弱性，并对脆弱性的严重程度进行评估，即对脆弱性被威胁利用的可能性进行评估，最终为其赋予相应等级值。在进行脆弱性评估识别时，提供的数据应该来自于这些资产的所有者或使用者，识别工作则应由来自于相关业务领域的专家参与进行。

2）脆弱性分类

脆弱性可以从技术和管理两个方面进行分类。技术脆弱性涉及物理层、网络层、系统层、应用层、管理层等各个层面的安全问题。管理脆弱性又可分为技术管理和组织管理两个方面。

脆弱性一般可以分为两大类，即资产本身的脆弱性和安全控制措施的不足。前者一般指操作系统漏洞、产品设计时安全方面的先天性不足等，这些是当前流行的漏洞扫描工具的强项，也是风险评估人员高度关注的问题。但是，一组资产所面临的问题，不能简单地累加。由于产品集成，引进了很多新的安全问题，例如对某些系统安全控制措施的不足。在目前注重组织整体业务的风险评估情况下，更不应该仅仅关注资产自身的脆弱性问题。

3）脆弱性赋值

可以根据资产损害程度、技术实现的难易程度、弱点流行程度，采用登记方式对已识别的脆弱性的严重程度进行赋值。脆弱性严重程度的等级划分为 5 级，分别代表资产脆弱性严重程度的高低，等级数值越大，脆弱性严重程度越高。脆弱性严重程度赋值表如表 5-12 所示。

表 5-12　脆弱性严重程度赋值表

等　级	标　识	定　义
5	很高	如果被威胁利用，将对资产造成完全损害
4	高	如果被威胁利用，将对资产造成重大损害
3	中	如果被威胁利用，将对资产造成一般损害
2	低	如果被威胁利用，将对资产造成较小损害
1	很低	如果被威胁利用，将对资产造成的损害可以忽略

4. 已有安全措施的确认

组织应对已有安全措施的有效性进行确认，对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少因安全事件发生对信息系统造成的影响，如业务持续性计划。

已有安全措施的确认与脆弱性识别存在一定联系。一般来说，安全措施的使用将减少脆弱性，但安全措施的确认并不需要像脆弱性识别过程那样具体到每个资产、组件的弱点，而是一类具体措施的集合。比较明显的例子是防火墙的访问控制策略，不必要描述具体的端口控制策略、用户控制策略，而只需要表明采用的访问控制措施。

5. 风险确定

1）风险计算原理

经过识别阶段后，采用适当的方法与工具，确定威胁利用脆弱性导致安全事件发生的可

能性，风险计算原理形式化可描述为

$$R = f(A,V,T) = f(I_a,L(V_a,T))$$

式中：R 表示风险；A 表示资产；V 表示脆弱性；T 表示威胁；I_a 表示资产的重要程度；V_a 表示资产本身的脆弱性；L 表示威胁利用资产的脆弱性造成安全事件发生的可能性。具体而言分为以下几个步骤。

（1）对资产的弱点进行排序。

（2）针对每一个弱点，确定可能利用此弱点造成安全事件威胁的类型。

（3）给确定的威胁赋值。

（4）将威胁值与脆弱点值相乘，得出安全事件发生的可能性，即安全事件发生的可能性$=L$（威胁可能性，脆弱点严重性）

（5）根据资产的重要程度以及安全事件发生的可能性计算风险值，即风险值$=f$（资产重要程度，安全事件发生的可能性）

6. 风险控制

确定安全风险等级后，就需要根据风险评估的结果进行相应的风险处理。处理方式包括以下 3 种。

1）降低风险

对于不能接受的风险，采取适当的控制措施，如系统安全加固、修补漏洞、人员培训等，减少风险发生的可能性，降低风险发生的影响。

2）避免风险

对于可以通过技术措施或管理/操作措施避免的风险，应当采取措施予以避免，如内外网隔离措施等。

3）接受风险

对于那些已采取措施予以降低或避免的风险，出于实际和其他方面的原因，其残余风险在组织接受的范围内，可以考虑接受风险。

5.3 小　　结

在信息时代，信息成为第一战略资源，起着至关重要的作用。因此，信息资产的安全是关系到企业能否完成其使命的大事。资产与风险是天生的一对矛盾，资产价值越高，面临的风险就越大。信息资产有着与传统资产不同的特性，面临着新型风险。信息安全风险管理的目的就是要缓解和平衡这一对矛盾，将风险控制到可接受的程度，保护信息及其相关资产，最终保证机构能够完成其使命。

信息安全风险评估是风险管理的重要组成部分，是信息安全工作中的重要一环。信息安全风险评估是对组织存在的威胁进行评估、对安全措施有效性进行评估以及对系统弱点被利用的可能性进行评估后的综合结果。良好和确切的风险评估是成功的信息安全风险管理的基础。

习　题

1. 简述信息安全风险管理与风险评估的概念。
2. 简述信息安全风险管理的内容。
3. 简述生命周期各个阶段中的信息安全风险管理。
4. 信息安全风险评估模型的风险要素有哪 3 类?
5. 简述风险评估中风险信息分析方法以及其优缺点。
6. 简述信息安全风险评估实施流程。

第6章　信息安全管理

本章学习目标：

- 了解信息安全管理的基本概念。
- 掌握信息安全管理的常用模型。

6.1　信息安全管理的基本概念

6.1.1　安全管理的概念

所谓管理，是指在群体活动中，为了完成一定的任务，实现既定的目标，针对特定的对象，遵循确定的原则，按照规定的程序，运用恰当的方法，所进行的制订计划、建立机构、落实措施、开展培训、检查效果和实施改进等活动。其中，管理的任务、目标、对象、原则、程序和方法是管理策略的内容，一系列的管理活动是在管理策略的指导下进行的。所以，首先要明确管理策略，然后才能开展管理活动。管理的概念组成如图6-1所示。

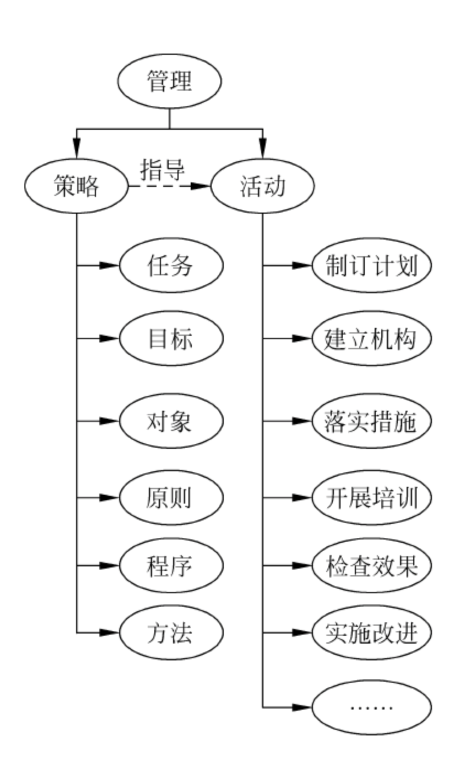


图6-1　管理的概念组成

安全管理是以管理对象的安全为任务和目标的管理。安全管理的任务是保证管理对象的安全。安全管理的目标是达到管理对象所需的安全级别，将风险控制在可以接受的程度。

信息安全管理是以信息及其载体——即以信息系统为对象的安全管理。信息安全管理的任务是保证信息的使用安全和信息载体的运行安全。信息安全管理的目标是达到信息系统所需的安全级别，将风险控制在用户可以接受的程度。信息安全管理有其相应的原则、程序和方法来指导和实现一系列的安全管理活动。管理、安全管理和信息安全管理的概念关系如图6-2所示。

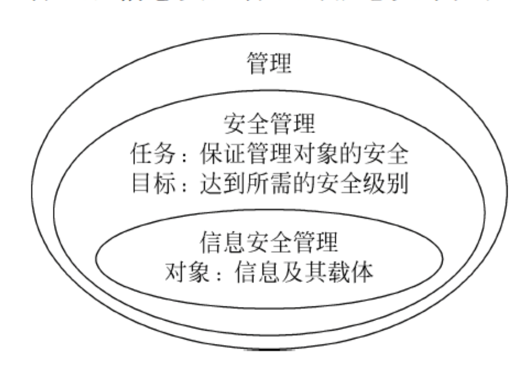


图6-2　管理、安全管理和信息安全管理的概念关系

6.1.2　安全管理的重要性

在信息时代，信息是一种资产。随着人们对信息资产利用价值认识的不断提高，信息资产的价值也在不断提升，信息安全的问题越发受到重视。针对各种风险的安全技术和产品不断涌现，如防火墙、入侵检测、漏洞扫描、病毒防治、数据加密、身份认证、访问控制、安全审计等，这些都是信息安全控制的重要手段，并且还在不断地丰富和完善。但是，却容易给人们造成一种错觉，似乎足够的安全技术和产品就能够完全确保一个组织的信息安全。其实不然，仅通过技术手段实现的安全能力是有限的，主要体现在以下两个方面。

(1) 许多安全技术和产品远远没有达到人们需要的水准。例如，微软公司的 Windows NT、IBM 公司的 AIX 等常见的企业级操作系统，大部分只达到了美国国防部 TCSEC C2 级安全认证，而且核心技术和知识产权都是国外的，不能满足国家涉密信息系统或商业敏感信息系统的需求。再如，在计算机病毒与病毒防治软件的对抗过程中，经常是在一种新的计算机病毒出现并已经造成大量损失后，才能开发出查杀该病毒的软件。也就是说，技术往往落后于新风险的出现。

(2) 即使某些安全技术和产品在指标上达到了实际应用的某些安全需求，但如果配置和管理不当，也不能真正地实现这些安全需求。例如，虽然在网络边界设置了防火墙，但出于风险分析欠缺、安全策略不明或系统管理人员培训不足等原因，防火墙的配置出现严重漏洞，其安全功效将大打折扣。再如，虽然引入了身份认证机制，但由于用户安全意识薄弱，再加上管理不严，使得口令设置或保存不当，造成口令泄露，那么依靠口令检查的身份认证机制会完全失效。

所有这些告诉人们一个道理，即仅靠技术不能获得整体的信息安全，需要有效的安全管理来支持和补充，才能确保技术发挥其应有的安全作用，真正实现整体的信息安全。俗话说“三分技术、七分管理”，就是强调管理的重要性，在安全领域更是如此。

信息安全管理的作用如下。

(1) 对组织的关键信息资产进行全面系统的保护，维持竞争优势。

(2) 在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度。

(3) 促使管理层贯彻信息安全管理体系，强化员工的信息安全意识，规范组织信息安全行为。

(4) 使组织的生意伙伴和客户对组织充满信心。

(5) 组织可以按照安全管理达到动态的、系统的、全员参与、制度化的、以预防为主的信息安全管理方式，用最低的成本达到可接受的信息安全水平，从根本上保证业务的持续性。

6.1.3　信息安全管理策略

信息安全管理策略应包括信息安全管理的任务、目标、对象、原则、程序和方法。

1. 信息安全管理的任务

信息安全管理的任务是保证信息的使用安全和信息载体的运行安全。信息的使用安全是通过实现信息的机密性、完整性和可用性这些安全属性来保证的。信息载体包括处理载体、传输载体、存储载体和入出载体，其运行安全就是指计算系统、网络系统、存储系统和外设系统能够安全地运行。

2. 信息安全管理的目标

信息安全管理的目标是达到信息系统所需的安全级别，将风险控制在用户可以接受的程度。

3. 信息安全管理的对象

信息安全管理的对象从内涵上讲是指信息及其载体——信息系统，从外延上说其范围由实际应用环境来界定。

4. 信息安全管理的原则

信息安全管理遵循如下基本原则。

1）策略指导原则

所有的信息安全管理活动都应该在统一的策略指导下进行。

2）风险评估原则

信息安全管理策略的制定要依据风险评估的结果。

3）预防为主原则

在信息系统的规划、设计、采购、集成和安装中要同步考虑信息安全问题，不可心存侥幸或事后弥补。

4）适度安全原则

要平衡安全控制的费用与风险危害的损失，注重实效，将风险降至用户可接受的程度即可，没有必要追求绝对的、高昂代价的安全，实际上也没有绝对的安全。

5）立足国内原则

考虑到国家安全和经济利益，安全技术和产品首先要立足国内，不能未经许可、未能消化改造直接使用境外的安全保密技术和产品设备，信息安全方面的关键技术和核心技术尤其如此。

6）成熟技术原则

尽量选用成熟的技术，以得到可靠的安全保证。采用新技术时要慎重，要重视其成熟程度。

7）规范标准原则

安全系统要遵循统一的操作规范和技术标准，以保证互连通和互操作，否则，就会形成一个个安全孤岛，没有统一的整体安全可言。

8）均衡防护原则

安全防护如同木桶装水，一是只要木桶的木板有一块坏板，水就会从里面泄漏出来；二是木桶中的水只和最低一块木板看齐，其他木板再高也无用。所以，安全防护措施要注意均衡性，注意是否存在薄弱环节或漏洞。

9）分权制衡原则

要害部位的管理权限不应交给一个人管理，否则，一旦出现问题将全线崩溃。分权可以相互制约，提高安全性。

10）全体参与原则

安全问题不只是安全管理人员的事情，全体相关人员都有责任。如果安全管理人员制定的安全制度和措施得不到相关人员的切实执行，安全隐患依然存在，安全问题就不会得到

真正解决。

11）应急恢复原则

安全防护不怕一万就怕万一，因此安全管理要有应急响应预案，并且要进行必要的演练，一旦出现问题就能够马上采取应急措施，阻止风险的蔓延和恶化，将损失减少到最低程度。

天灾人祸在所难免，因此在灾难不能同时波及的地区设立备份中心，保持备份中心与主系统数据的一致性。一旦主系统遇到灾难而瘫痪，便可立即启动备份系统，使系统从灾难中得以恢复，保证系统的连续工作。

12）持续发展原则

为了应对新的风险，对风险要实施动态管理。因此，要求安全系统具有延续性、可扩展性，能够持续改进，始终将风险控制在可接受的水平。

5. 信息安全管理的程序

信息安全管理的程序遵循 PDCA 循环模式的 4 大基本步骤。

(1) 计划(plan)。制订工作计划，明确责任分工，安排工作进度，突出工作重点，形成工作文件。

(2) 执行(do)。按照计划展开各项工作，包括建立权威的安全机构、落实必要的安全措施、开展全员的安全培训等。

(3) 检查(check)。对上述工作所构建的信息安全管理体系进行符合性检查，包括是否符合法律法规的要求，是否符合安全管理的原则，是否符合安全技术的标准，是否符合风险控制的指标，等等，并报告结果。

(4) 行动(action)。依据上述检查结果，对现有信息安全管理策略的适宜性进行评审与评估，评价现有信息安全管理体系的有效性，采取改进措施。

6. 信息安全管理的方法

信息安全管理根据具体管理对象的不同，采用不同的具体管理方法。信息安全管理的具体对象包括机构、人员、软件、设备、介质、涉密信息、技术文档、网络连接、门户网站、应急恢复、安全审计、场地设施等。

6.1.4 信息安全管理体系

信息安全管理发展至今，人们越来越认识到安全管理在整个企业运营管理中的重要性，而作为信息安全管理方面最著名的国际标准——ISO/IEC 27001，则成为可以指导现实工作的最好参照。

ISO 27001 目前作为国际标准，正迅速被全球所接受。依据 ISO 27001 标准进行信息安全管理体系建设，是当前各行业组织在推动信息安全保护方面最普遍的思路和正确的决策。

ISO 27001 为组织建立、实施、维护和持续改进信息安全管理体系(ISMS)提出相关要求。采用 ISMS 是组织的一项战略决策。组织 ISMS 的设计和实施受组织的战略决策、组织需求、目标、安全需求以及工作流程和组织规模等因素的影响。上述因素会随着时间的推移而不断发生变化。

信息安全管理体系通过实施风险管理过程来保护组织信息的机密性、完整性和可用性，对风险进行充分的管理并为相关方带来信心。

1. ISMS 标准

组织应在其整体业务活动中且在所面临风险的环境下建立、实施、运行、监视、评审ISMS，形成文件，并保持和改进其有效性文档化的ISMS。

2. 建立和管理 ISMS

组织应做以下方面的工作。

(1) 根据业务、组织、位置、资产和技术等方面的特性，确定ISMS的范围和边界，包括对范围任何删减的详细说明和正当理由。

(2) 根据业务、组织、位置、资产和技术等方面的特性，确定ISMS方针。ISMS方针应包括以下内容。

① 包括设定目标的框架和建立信息安全工作的总方向和原则。

② 考虑业务和法律法规的要求及合同中的安全义务。

③ 在组织的战略性风险管理环境下，建立和保持ISMS。

④ 建立风险评价的准则。

⑤ 获得管理者批准。

(3) 确定组织的风险评估方法。

① 识别适合ISMS、已识别的业务信息安全和法律法规要求的风险评估方法。

② 制定接受风险的准则，识别可接受的风险级别。选择的风险评估方法应确保风险评估产生可比较的和可再现的结果。

(4) 识别风险。

① 识别ISMS范围内的资产及其责任人。

② 识别资产所面临的威胁。

③ 识别可能被威胁利用的脆弱性。

④ 识别丧失保密性、完整性和可用性可能对资产造成的影响。

(5) 分析和评价风险。

① 在考虑丧失资产的保密性、完整性和可用性所造成的后果的情况下，评估安全失效可能造成的影响。

② 根据主要的威胁和脆弱性、对资产的影响以及当前所实施的控制措施，评估安全失效发生的现实可能性。

③ 估计风险的级别。

④ 确定风险是否可接受，或者是否需要在使用中对所建立的接受风险的准则进行处理。

(6) 识别和评价风险处理的可选措施，可能的措施如下。

① 采用适当的控制措施。

② 在明显满足组织方针策略和接受风险准则的条件下，有意识地、客观地接受风险。

③ 避免风险。

④ 将相关业务风险转移到其他方，如保险、供应商等。

(7) 为处理风险选择控制目标和控制措施。

控制目标和控制措施应加以选择和实施，以满足风险评估和风险处理过程中所识别的要求。这种选择应考虑接受风险的准则、法律法规以及合同要求。

(8) 获得管理者对建议的残余风险的批准，获得管理者对实施和运行 ISMS 的授权。

(9) 准备适用性声明(Statement of Applicability，SoA)。应从以下几方面准备适用性声明。

① 所选择的控制目标和控制措施以及选择的理由。

② 当前实施的控制目标和控制措施。

③ 对任何控制目标和控制措施的删减，以及删减的合理性说明。

3. 实施和运行 ISMS

(1) 为管理信息安全风险识别适当的管理措施、资源、职责和优先顺序，即制订风险处理计划。

(2) 实施风险处理计划以达到已识别的控制目标，包括资金安排、角色和职责的分配。

(3) 实施所选择的控制措施，以满足控制目标。

(4) 确定如何测量所选择的控制措施或控制措施集的有效性，并指明如何用这些测量措施来评估控制措施的有效性，以产生可比较的和可再现的结果。

(5) 实施培训和意识教育计划。

(6) 管理 ISMS 的运行。

(7) 管理 ISMS 的资源。

(8) 实施能够迅速检测安全事态和响应安全事件的规程和其他控制措施。

4. 监视和评审 ISMS

(1) 执行监视与评审规程和其他控制措施，以达到如下目的。

① 迅速检测过程运行结果中的错误。

② 迅速识别试图的和得逞的安全违规和事件。

③ 使管理者能够确定分配给人员的安全活动或通过信息技术实施的安全活动是否按期望执行。

④ 通过使用指示器，帮助检测安全事态并预防安全事件。

⑤ 确定解决安全违规的措施是否有效。

(2) 在考虑安全审核结果、事件、有效性测量结果、所有相关方的建议和反馈的基础上，进行 ISMS 有效性的定期评审(包括满足 ISMS 方针和目标，以及安全控制措施的评审)。

(3) 测量控制措施的有效性以验证安全要求是否被满足。

(4) 按照计划的时间间隔进行风险评估的评审，以及对残余风险和已确定的、可接受的风险级别进行评审，应考虑以下变化。

① 组织。

② 技术。

③ 业务目标和过程。

④ 已识别的威胁。

⑤ 已实施的控制措施的有效性。

⑥ 外部事态,如法律法规环境的变更、合同义务的变更和社会环境的变更。

(5) 按计划的时间间隔,实施ISMS内部审核。内部审核有时称为第一方审核,是用于内部目的、由组织自己或以组织的名义所进行的审核。

(6) 定期进行ISMS管理评审,以确保ISMS范围保持充分、ISMS过程的改进得到识别。

(7) 考虑监视和评审活动的结果,以更新安全计划。

(8) 记录可能影响ISMS的有效性或执行情况的措施。

5. 保持和改进ISMS

(1) 实施已识别的ISMS改进。

(2) 采取合适的纠正和预防措施。从其他组织和组织自身的安全经验中吸取教训。

(3) 向所有相关方沟通措施和改进情况,其详细程度应与环境相适应,必要时商定如何进行。

(4) 确保改进达到了预期目标。

6. 文档要求总则

文档应包括管理决定的记录,以确保所采取的措施符合管理决定和方针策略,还应确保所记录的结果是可重复产生的。重要的是,能够显示出所选择的控制措施回溯到风险评估和风险处理过程的结果,并进而回溯到ISMS方针和目标之间的关系。

7. 管理承诺

管理者应通过以下活动,对建立、实施、运行、监视、评审、保持和改进ISMS的承诺提供证据。

(1) 制定ISMS方针。

(2) 确保ISMS目标和计划得以制订。

(3) 建立信息安全的角色和职责。

(4) 向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性。

(5) 提供足够资源,以建立、实施、运行、监视、评审、保持和改进ISMS。

(6) 决定接受风险的准则和风险的可接受级别。

(7) 确保ISMS内部审核的执行。

(8) 实施ISMS的管理评审。

8. 纠正措施

组织应采取措施,消除与ISMS要求不符合的原因,并防止再发生。形成文档的纠正措施规程,应规定以下要求。

(1) 识别不符合ISMS的要求。

(2) 确定不符合ISMS的要求的原因。

(3) 评价确保不符合ISMS的要求不再发生的措施需求。

(4) 确定和实施所需要的纠正措施。

(5) 记录所采取措施的结果。

(6) 评审所采取的纠正措施。

9. 预防措施

组织应确定预防措施,以消除潜在不符合 ISMS 的原因,防止其发生。预防措施应与潜在问题的影响程度相适应。形成文档的预防措施规程,应规定以下方面的要求。

(1) 识别潜在的不符合 ISMS 的要求及其原因。

(2) 评价防止不符合 ISMS 的要求发生的措施需求。

(3) 确定和实施所需要的预防措施。

(4) 记录所采取措施的结果。

(5) 评审所采取的预防措施。

6.2 信息安全管理模型

信息安全管理有多种模型或模式,各种模型是从不同角度构建的,都有各自特别适用的范围或对象,但各种模型所提出的安全管理概念都有利于对信息安全管理的原理和实践进行理解。归纳起来,目前比较流行的模型有以下 4 种。

(1) 安全要素关系模型。

(2) 风险要素关系模型。

(3) 基于过程的风险管理模型。

(4) PDCA 模型。

上述概念模型和组织的业务目标一起可形成一个对组织的信息安全目标、方针和策略的安全管理轮廓。信息安全的整体目标就是保证组织的信息系统能够安全地运行,并且将风险控制在可以接受的程度。任何安全措施都不是万能的,也不是对任何风险完全有效的,因此需要规划和实施预防意外事件的数据备份或系统备份,以及事件发生后的恢复计划,构建可将损坏程度限制在一定范围的安全保障体系。

6.2.1 安全要素关系模型

信息系统安全是一个需要从不同方面来观察和研究的多维问题。为了确定和实现一个全局的、一致的信息安全方针和策略,一个组织应该考虑与之相关的所有方面的问题。安全要素之间的关系说明了资产可能受大量潜在威胁的情况,如图 6-3 所示。一般来说,这些威胁的集合总是随时间变化的,并且只有部分是已知的或可预见的。

这一模型表示的含义如下。

(1) 环境、约束和威胁,其中环境情况和约束条件是相对稳定的,其变化是可以预见的,而威胁则是动态变化的,并且只有部分是已知的或者是可预见的。

(2) 应予以保护的组织的信息系统资产及其价值。

(3) 这些资产存在的脆弱性。

(4) 为保护资产、消除或减少脆弱性、降低风险所选择的安全保护措施。

(5) 评估可接受的残留风险。

如图 6-3 所示,一些安全措施(S)可以在降低与多种威胁(T)和多种脆弱性(V)相关联的风险(R)中起作用。有时需要几种安全措施才能保证残留风险(RR)是可接受的。在残

留风险经过评估并认为是可接受的情况下,即使出现威胁,也没必要采取额外的安全措施,但应加强监视;在另外一些情况下可能存在某种脆弱性,但没有已知的威胁利用它,可以采用一些安全措施来监视威胁实施的环境,以确保没有威胁能开发或利用该脆弱性。模型中的约束(C)可以影响安全措施的选择。

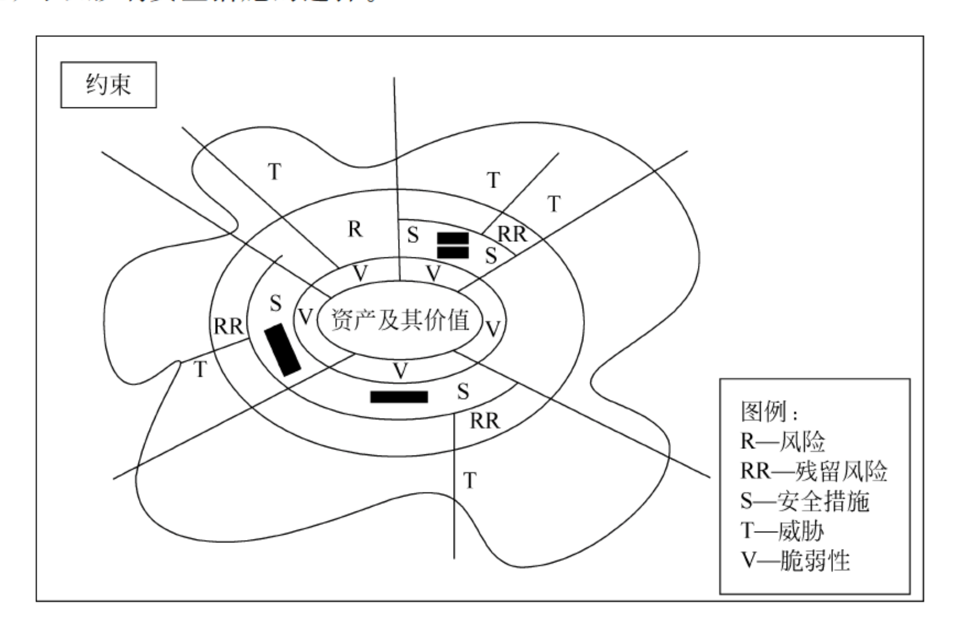


图 6-3 安全要素之间的关系

这一概念模型展示了需保护的信息系统资产及其价值与脆弱性、威胁、风险、残留风险以及环境和约束等安全要素之间的关系,提供了一种围绕资产及其价值进行安全管理的思路。

6.2.2 风险要素关系模型

风险要素关系模型阐述了与风险相关的安全要素之间的关系,如图 6-4 所示。为了展示得简单清晰,这里只表示了主要关系。

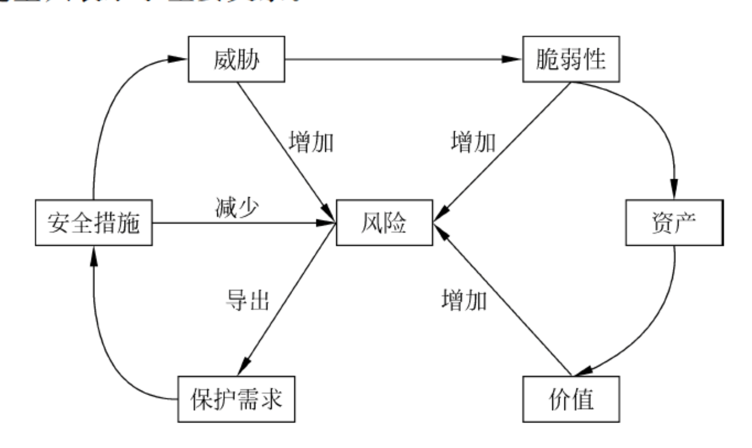


图 6-4 风险要素关系模型

信息系统的资产可能存在风险,例如信息的泄露、未经授权的修改、不可用和抵赖,信息服务的不可用或能力降低等。对于这些风险,首先要识别出资产的真实价值,然后要考虑哪些威胁可能会造成影响,进一步,反过来考查哪些脆弱性可能会被这些威胁利用、造成影响

以及它们发生的可能性有多大。根据资产的价值、脆弱性的严重程度以及威胁的等级确定出风险大小。对风险的识别和度量能够导出整个安全保护的需求，并通过安全措施的实施来满足。安全措施的实施可以对抗威胁，并减少风险。

这一概念模型从风险要素之间的逻辑关系方面提供了围绕风险要素进行安全管理的思路。这一模型与图 6-3 所示的模型比较，在风险控制成本与被保护的资产之间考虑了平衡。

图 6-5 和图 6-6 分别说明了资产、保护需求与威胁、脆弱性之间的逻辑关系。

图 6-5 说明保护需求源于资产及其价值，重点考虑了威胁利用资产的脆弱性对资产构成的风险情况，三者之间建立了在考虑威胁因素情况下关于保护需求与资产价值的平衡关系。



图 6-5　资产、保护需求与威胁的关系示意

图 6-6 说明保护需求源于资产及其价值，重点考虑了由于资产脆弱性引起的风险情况，三者之间建立了在考虑资产脆弱性情况下关于保护需求与资产价值的平衡关系。



图 6-6　资产、保护需求与脆弱性的关系示意

6.2.3　基于过程的风险管理模型

基于过程的风险管理是一个由许多子过程组成的系统工程。其中一些过程，例如配置管理和变更管理，可以用来控制安全以外的其他过程。经验表明，过程风险管理及其风险分析子过程在信息安全管理中极其有用。图 6-7 说明了基于过程的风险管理的几个方面，包括风险分析、变更管理、配置管理和风险调控等。

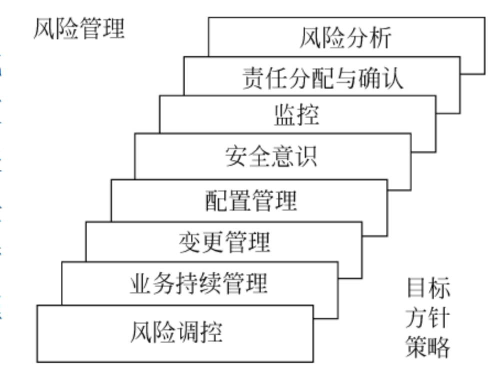


图 6-7　基于过程的风险管理

风险管理是一个基于可接受成本的、对影响信息系统安全的风险进行识别、控制、最小化或消除过程。风险管理根据评估的风险与保护效能和保护成本的比较，综合考虑不同类型的安全措施及配置这些措施所花费的代价以及从保护中获得利益之间的平衡关系，然后制定出与组织的信息安全策略和业务目标相一致的信息系统安全方针和实现策略。安全措施的选择与风险有关。可接受的残留风险的等级是风险评估的基础。重要的是，要在识别和实现安全措施过程中对所耗费的最小成本和组织所拥有的资源价值之间取得平衡，也就是说信息系统的安全保护要适度。

风险管理是一系列渐进的活动。对于新系统或者计划阶段中的系统来说，要准备将风险管理贯穿到设计、开发和系统运维过程中。对于已经存在的系统，应该适时引入风险管

理。而当计划对系统进行重大变更时,风险管理应该成为这一变更计划的一部分。风险管理应该考虑一个组织中的所有信息处理系统,而不应该孤立地应用到某一个系统。同时特别强调,安全措施本身也可能包含脆弱性,进而可能导致新的风险。因此在设计或者选取安全保护措施时,要注意不因采取新的安全措施而引入新的安全脆弱性,从而导致新的风险,故选择安全措施必须小心,要做到在减少风险的同时,不引进新风险。

风险分析是对那些需要被控制或被接受的风险进行识别。信息系统的风险分析涉及对资产价值、脆弱性和威胁以及威胁的后果进行综合分析。风险是通过对机密性、完整性、可用性、可靠性、抗抵赖及可确认性的可能损坏进行识别和分析的。

责任分配与确认是风险管理中的一种重要的措施,它明确无误地将责任进行分配并确定责任者。因此,资产的所有权和相关的安全责任人加上对安全行为的审计,可以回溯并追究安全事件的责任,以此增强相关人员的安全意识,并对来自内部或外部的恶意行为人构成威慑,这对信息系统的安全来说非常重要。

监控是实施安全措施所需要的,安全措施本身的监控功能则能确保安全功能正常发挥作用。在安全设备运行期间,当环境改变后,监控功能应仍能维持所设计的功能。系统日志的自动审核和分析是帮助系统性能达到预期效果的有效工具。这些工具也可以用来检测有害事件,并可以对某些潜在威胁起到威慑的作用。

需要定期验证安全措施是否保持了设计的效能。通过监控和对安全效能符合性的检测可以确定安全措施正常发挥功效。很多安全措施会产生输出,例如日志、报警信息等。通过检查这些输出信息可以发现安全事件和分析潜在的安全事件。系统审计功能可以在安全管理方面提供有用的信息,并能提供监控所需的输入信息。

安全意识是确保信息系统安全所需的基本要素。组织中的有关人员缺乏安全意识以及不规范或不良的操作习惯会极大地降低安全措施的有效性或者引发风险。一个组织中的操作人员通常被认为是信息安全链中的薄弱环节之一。为确保组织中的每个人都有足够的安全意识,非常有必要建立和维持有效的安全意识培训规程。建立这个规程的主要目的是向员工、合作伙伴、供应商阐明以下内容。

(1) 安全目标、安全方针和策略。

(2) 与他们的角色和责任相关的操作规范要求。

(3) 从职业道德和行政、技术规范上需要养成良好习惯和必须遵从的行为准则。

此外,安全培训规程还应提供规范员工、合作伙伴和供应商在安全保障体系中承担的安全责任和义务的内容。

应使组织内从高层管理人员到负责日常事务的员工都知晓并贯彻实施安全意识规程。通常需要针对组织中不同部门的人、不同的角色以及负不同责任的人制作相应的安全意识教育材料。一个比较合理的综合性的安全意识规程培训是分阶段完成的。每个阶段的培训内容都以以前的经验为基础,从安全的概念开始到如何解决出现的安全问题。

组织内的安全意识教育规程可以包括各种各样的活动,其中一项活动是安全意识教育材料的制作和发布;另一项活动是举办训练课程,对所有员工有针对性地进行合适的安全技术和实践培训。此外,训练课程还应提供若干特定安全专题方面的具有专业水准的讲座。

一般来说,在业务培训计划中加入安全知识是行之有效的。对于安全意识培训规程的制定需要考虑以下问题。

(1) 培训需求分析。

(2) 培训课程的开发与提交。

(3) 对培训规程执行情况的监控。

(4) 安全意识培训规程的内容。

配置管理或控制是启动并维持系统参数配置的过程,以正式或非正式的方式完成。配置管理的基本安全目标是确保及时获得信息系统变更后所需的安全运行参数和安全控制参数配置表,以不降低安全措施效能和组织的整体安全的方式对已批准的系统变更进行安全管理。

变更管理是另外一种过程——当一个信息系统发生变更时用来帮助识别新的安全管理需求。信息系统及运行环境经常发生变化,这些变化或者是由新的信息系统特性和服务所导致的,或是因为发现新的脆弱性和威胁。信息系统的变更包括以下内容。

(1) 运行环境。

(2) 新的程序。

(3) 新的功能和性能。

(4) 软件升级。

(5) 硬件更换。

(6) 新增用户,包括外部用户组或匿名组。

(7) 增加子网或增加与外部网络互联。

(8) 新的脆弱性或威胁出现。

当信息系统发生变动或者计划变动信息系统时,重要的是确定这些变动会对系统安全带来的影响。如果系统拥有配置控制中心或者其他组织机构来管理系统的技术变动,那么应指定信息系统安全员并赋予其相应的职责,以便对这些变动是否会影响系统的安全以及影响的程度做出判断。在某些情况下,需要对变动可能降低系统安全的原因进行分析,这时往往需要评估安全性降低的程度,并基于所有有关的事实做出管理决策。换句话说,改变一个系统需要适时地考虑对安全的影响。对于涉及购买新的硬件、软件或服务的重大改变,需要分析以确定新的安全需求。另一方面,许多变动只造成小的系统性能变化,不需要像发生结构性变动那样做深入的分析。然而,不管系统变动大或小都需要进行风险评估,确定保护收益与成本之间的平衡。

业务持续性管理是维持业务不间断的管理过程,它为确保业务的连续运营提供进程和资源的持续可用性。业务持续管理还包括应急计划和灾难恢复。

应急计划是当信息系统运行和维持能力降低或系统不可用时如何维持或快速恢复基本运行业务的保证。这些计划应当涉及以下各种可能的情况。

(1) 规定各种业务容忍中断的时间,通常以小时或分计算。

(2) 预估不同类型设施所受的损失。

(3) 估计建筑物及其附属设施所受的总损失。

(4) 恢复到损失发生前状态所需的时间。

灾难恢复计划描述怎样使受安全事件影响的信息系统恢复运行。灾难恢复计划包括以

下内容。

(1) 制定灾难的识别准则。

(2) 确定恢复计划的职责。

(3) 履行恢复计划的职责。

(4) 恢复活动的过程描述。

(5) 测试恢复计划是否有效。

风险调控过程贯穿于安全工程的整个生命周期。图 6-8 说明了风险调控的各个环节及其调控流程。

这一模型的优点是强调了基于风险调控的各个阶段,具有一定的可操作性;缺点是对于各个阶段之间的关系没有给出具有逻辑性的描述。

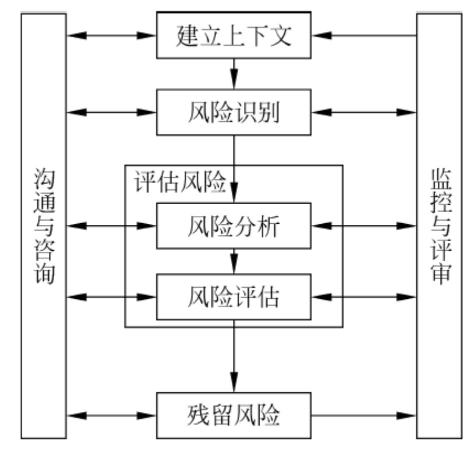


图 6-8 风险调控过程概览

6.2.4 PDCA 模型

PDCA 循环是美国质量管理专家休哈特博士首先提出的,由戴明采纳、宣传并获得普及,所以又称戴明环。全面质量管理的思想基础和方法依据就是 PDCA 循环。PDCA 循环的含义是将质量管理分为 4 个阶段,即计划(plan)、执行(do)、检查(check)、行动(action)。在质量管理活动中,要求把各项工作按照做出计划、计划实施、检查实施效果,然后将成功的纳入标准,不成功的留待下一循环去解决。这一工作方法是质量管理的基本方法,也是企业管理各项工作的一般规律。PDCA 过程模型如图 6-9 所示。

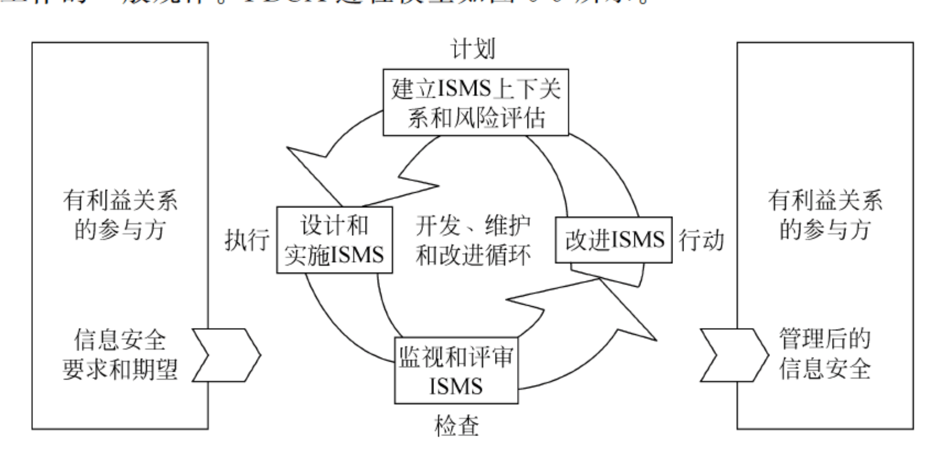


图 6-9 PDCA 过程模型

1. 计划——对组织的信息安全进行总体规划

建立 ISMS 的结构关系,提出信息安全目标、方针和策略。其中,安全目标是一个满足组织对信息系统安全要求的指标体系;安全方针是达到安全目标的方法和途径;安全策略是实现安全目标的一系列规则和指令。

2. 执行——设计和实施 ISMS

对实现信息安全目标所需的过程程序进行设计和工程实现。

3. 检查——监控和评审 ISMS

采用自动工具和人工检测结合的方法,根据安全目标、方针、策略和运行实践情况对

过程程序的安全性能进行监控和评审，并给出与安全要求指标是否符合的定量或定性的结论。

4. 行动——改进 ISMS

改进过程程序的安全性能，使之符合安全规划中提出的安全要求指标。

6.3　基于 PDCA 的信息安全管理实践

以上提到的几种信息安全管理模型都是从不同角度或根据不同应用领域的需要设计的，都有一定的参考价值，对于理解和认识信息安全管理可以起到“敲门砖”的作用。在面对具体的信息安全管理问题时，建议读者不要盲目套用，而应自己用信息安全管理理论和方法设计符合实际需要的信息安全管理模型。

本节主要根据 PDCA 安全模型的一些参考对一个简单的网络售票系统的信息安全管理过程做一些分析与探讨。

6.3.1　背景分析

当今社会信息技术飞速发展，人们的生活越来越多地依靠网络。网络售票系统出现之后大大方便了人们的出行，其信息安全管理也成了一个需要考虑和研究的问题。该分析主要针对一个网络售票系统的信息安全管理，根据 PDCA 安全管理模型，提出该系统信息安全管理的方案。该网络售票系统包括一个售票服务器、一个数据库，以及客户端。主要进行的业务是客户通过客户端注册信息，通过网络购买火车票。

6.3.2　前期分析

1. 安全需求分析

1）信息安全范围需求

确保整个系统运行的信息安全，主要涉及以下几方面。

（1）信息，包括用户数据、通信数据、票务数据等。

（2）硬件、软件。

（3）人员管理。

2）信息安全优先级需求

信息安全优先级从高到低的顺序依次是关键岗位人员、关键信息、硬件、软件。

考虑的原因：关键岗位人员掌握着核心信息，这一部分可能对于安全造成毁灭性的影响；关键信息，如系统的管理员密码、密钥等，对整个系统的数据安全有很大影响；硬件的损坏对系统的安全也有较大影响；相对于其他几个，系统的软件对于整个系统的影响稍小。

2. 潜在风险分析

1）内部风险

关键人员对于自己掌握的关键信息的泄露，使得购票系统信息的安全处于危险之中。例如，通信密钥的泄露导致加密信息丧失机密性；硬件的损坏导致系统崩盘或信息丢失。

2）外部风险

来自外部的攻击，侵入系统获取用户信息、票务信息或对信息进行破坏；系统人员操作失误导致信息丢失；用户客户端与服务器端通信过程中通信信息的泄露。

6.3.3 PDCA 实施

1. 计划

1）数据安全

主要是计划保护数据信息的机密性、完整性、可用性，即信息安全中的 CIA 性质。

（1）数据库数据。由于是火车票的售票系统，用户数据包括用户的实名制信息，以及其他敏感的个人信息，票券信息都保存在数据库中，需要保证其机密性，所以应将数据库中的信息进行加密保存，并且保证数据库的安全，防止 SQL 注入攻击。

数据库信息量比较大，采用非对称密码进行加密，虽然安全，但是加密速度很慢。由于是网络售票系统，许多信息需要及时处理，这时可能需要提取数据库的信息，如果加解密速度过慢，可能导致系统响应时间过长，不符合实际实施。因此使用对称加密的方式，实施时使用的加密算法为 DES(Data Encryption Standard，数据加密标准)算法。它是一种使用密钥加密的算法，安全性较好，且加密速度比较快，能够很好地满足需求。

数据库安全的保证主要通过设置数据库的登录验证口令，编写数据库时规范数据库语句，查询时使用存储过程，进行输入验证等来防止 SQL 注入攻击。关键的数据库口令、管理员登录口令等要求一定长度，并按一定的期限进行更换。

（2）通信数据安全。用户与服务器进行购票通信过程中，可能会发送重要的个人信息，在支付过程中，可能要交换银行卡信息，所以需要保护其机密性，需要通过安全的通信信道传输，另外数据通信要保证其完整性，所以使用消息校验。

用户通信数据安全主要利用 SSL 协议提供的安全通信信道。SSL 协议是为网络通信提供安全及数据完整性的一种安全协议，通信双方通过协商的加密密钥对通信信道进行加密，在加密的通信信道上进行信息的传输，保证信息机密。信息的完整性则通过哈希算法来实现，通过比对信息的哈希值，确认信息的完整性。

（3）数据备份与恢复。这个主要考虑的是数据的可用性。有时可能发生异常造成数据的损坏、丢失，通过备份的数据来保证信息的可用性。这里主要是建立一个备份数据库，以便在需要时进行数据恢复。

2）人员管理

制定相关的一套规定来对人员进行管理，并严格按照规定执行，保证人员这一方面的安全，包括人员的选择、培训等。

3）硬件安全

制订详细的硬件管理方案，合理管理和使用硬件，及时排查小故障和小问题，保证硬件正常运行。主要是对硬件的备案与定期检查，还可以利用物联网技术进行监测。

4）防攻击

建立防火墙、入侵检测系统，防止一些可能的系统攻击，并建立有效的入侵检测机制，及时监视发现系统的异常。利用防火墙阻止可能的攻击，利用入侵检测系统检测记录入侵即可能入侵的行为，并提醒管理员。

5）事故应急

制订一个可行的事故应急方案，当事故发生时，根据方案进行相应的应急处理，保证事故不会对系统造成影响，同时也保证系统的安全，不至于造成损失。

事故按严重程度由低到高分为两级：一级事故如硬件普通故障、系统遭到攻击、数据库数据少量错误等，由相关的管理人员进行检查处理即可；二级事故如系统遭到入侵，用户数据丢失，数据库数据大量泄露、丢失，系统主密钥泄露、关键口令泄露等，故需要通知相关的信息安全管理部门进行处理，寻找问题，并尽快解决。

2. 实施

这里简单描述上述项目在具体情境的实现。

1）数据安全

(1) 数据库信息。当一个信息写入数据库时，使用系统主密钥进行加密。当然不是对所有信息进行加密，只对重要信息进行加密，如用户信息、密码信息等。当需要提取数据库信息进行使用时，系统利用主密钥解密信息，再进行正常使用。数据库管理员需要使用口令进行登录，使用的口令到期则须重换。

(2) 通信数据。服务器与用户进行交互，首先进行会话，建立起 SSL 安全信道，利用密钥进行加密，然后用户与服务器进行通信。

(3) 数据备份与恢复。每次数据写入数据库时，同时也写入一份到备份数据库。当检测数据时发现数据损坏，则从备份数据库重新读入数据。当发生数据大量流失时，应使用备份数据库数据。

2）人员管理

若一个人员作为系统管理员上岗，则对其进行培训，一方面保证其能够正确操作，另一方面也对其进行保密教育；在职时期，对其进行监管，要求其严格遵守规定；当这个管理员离职时，再进行离职培训，进行一些保密协定。离职后处理其账号，注销或更改信息。

3）硬件安全

专门的硬件工作部门定期对系统硬件进行检查记录，每次检查进行小故障的排除并备案。例如，检查员发现了一处电路线路老化，应及时进行修复并且备案。

4）防攻击

当有人向售票系统发起攻击时，防火墙阻止其入侵行为，入侵检测系统则记录该行为，提醒管理员检查系统。

3. 检查

这一阶段主要是对前一阶段的实施进行检查，以发现问题。评估小组使用一些方法对系统进行检测，如使用问题记录、情景模拟、渗透测试等。问题记录是对出现的问题进行记录，如果同一个问题频繁出现，则需要引起警觉；情景模拟是通过对相应情景的设想进行分析讨论与验证，去发现问题；渗透测试是聘请专业的团队，对系统进行攻击和检测，以获取可能存在的未知漏洞，即使用攻击来检验防守的原理，但在进行时要注意不能对系统的正常功能造成影响，或给系统造成不可挽回的损失。

通过对前一过程的检查发现数据通信中的问题。购买火车票是一个实名制的过程，没有进行身份验证，用户可能会被假冒，从而给用户和服务商都带来损失。另外通信加密密钥

的交换不安全,密钥可能会被截获;密钥的安全管理也没有考虑。这些问题都有可能在实际过程中造成信息泄露。

4. 行动

这一阶段主要是对前一阶段发现的问题进行解决,如果不能解决则加入下一次 PDCA 循环。

针对发现的问题,在用户通信过程中要添加一个非对称密码算法来用作身份认证。非对称密码的特性使其有独特的身份认证优势。RSA 算法是非对称密码的代表,是基于大整数分解的数学难题,具有很好的安全性。服务器用自己的私钥加密一个时间信息发给客户端用户,客户端使用公钥进行解密,由于公钥来自于可信的第三方机构,解密成功则客户端验证服务器身份成功;服务器端对客户端的验证则是用户使用自己的私钥加密时间信息发给服务器端,服务器端用公钥解密验证。另外,非对称密码的引入也方便了密钥交换。而密钥管理则是引入一个密钥管理中心来解决,该中心负责密钥的保护与管理。

6.4 小 结

“堵漏洞、做高墙、防外攻”是长期以来网络信息安全的基本状况。当人们讨论网络信息安全的时候,往往只关心黑客和操作系统的漏洞,尽管它们是安全的重要部分,但只是安全广义概念上的两个组件而已。

保障信息安全有 3 个路径:技术、管理、法律法规。而日常提及信息安全时,更多是在与技术相关的领域,例如入侵检测技术、防火墙技术、防病毒技术、加密技术、CA 认证技术等。这是因为信息安全技术和产品的采纳,能够快速见到直接效益。

信息安全作为一个动态发展的过程,已经成为一项系统化的工程。每个信息系统及网络环境都有一定程度的漏洞和风险,仅从纯粹的技术并仅仅依赖于安全产品的堆积来应对迅速发展变化的各种攻击手段是不能持续有效的,绝对的信息安全是不存在的。人们总在反思自身技术的不足,而却忽视了另外两个层面——管理和法律法规上的保障。应该从信息安全决策管理、风险管理、安全策略管理及应急服务等方面探讨提升信息安全管理的水平,从而提高对信息安全的保障。

习 题

1. 什么是信息安全管理?
2. 什么是信息安全管理体系?
3. 简述 PDCA 模型。
4. 请阐述主要的信息安全管理模型。

第 7 章　安全层次划分

本章学习目标：

- 了解安全层次的概念。
- 了解并掌握各个层面上的安全解决方案。

安全体系的建设涉及安全的各个层面，通常应该从应用安全、系统安全、网络安全、安全协议及安全的密码算法等方面来寻求解决方案。

7.1　安全的密码算法

7.1.1　密码算法安全性概述

加密技术是对信息进行编码和解码的技术。编码是把原来的可读信息(又称明文)译成代码形式(又称密文)，其逆过程就是解码(解密)。加密技术的要点是加密算法。加密算法可以分为对称加密、非对称加密和不可逆加密 3 类算法。

理论上大部分的算法基本上都是可以破解的，只是需要很多台计算机并行运算很长时间才能破解。密钥越长，需要耗费的资源越多，以此来提高破解的成本，由于成本过高导致不进行攻击或采用旁道攻击。同时密钥越长，加解密的成本也会随之提高，所以可以根据信息的价值和保密要求来选择合适的算法。

常用的安全加密算法如下所述。

(1) DES(Data Encryption Standard，数据加密标准)：对称算法，速度较快，适用于加密大量数据的场合。

(2) 3DES(Triple DES，3 重 DES)：是基于 DES 的对称算法，对一块数据用 3 个不同的密钥进行 3 次加密，强度更高。

(3) RC2 和 RC4：对称算法，用变长密钥对大量数据进行加密，比 DES 快。

(4) IDEA(International Data Encryption Algorithm，国际数据加密算法)：使用 128 位密钥提供非常强的安全性。

(5) AES(Advanced Encryption Standard，高级加密标准)：属于对称算法，是下一代加密算法标准，速度快，安全级别高，现在 AES 的一个实现是 Rijndael 算法。

(6) RSA：由 RSA 公司发明，是一个支持变长密钥的公共密钥算法，需要加密的文件块的长度也是可变的，属于非对称算法。

(7) DSA(Digital Signature Algorithm，数字签名算法)：是一种标准的 DSS(数字签名标准)，严格来说不算加密算法。

(8) BLOWFISH：使用变长的密钥，长度可达 448 位，运行速度很快。

(9) MD5：严格来说不算加密算法，只能说是摘要算法。MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出

由4个32位分组组成,将这4个32位分组级联后将生成一个128位散列值。

(10) PKCS(The Public-Key Cryptography Standards):是由美国RSA数据安全公司及其合作伙伴制定的一组公钥密码学标准,其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。

(11) SSF33、SSF28、SCB2(SM1):国家密码局的隐蔽不公开的商用算法,在国内的民用和商用中,除这些不允许使用外,其他的都可以使用。

(12) 其他算法:ElGamal、Diffie-Hellman、新型椭圆曲线算法ECC等。

加密算法的安全级别如表7-1所示。

表7-1 加密算法的安全级别

安全级别	算法复杂度	算　　法
薄弱(weak)	$O(2^{40})$	DES,MD5
传统(tradition)	$O(2^{64})$	RC4,SHA-1
基准(baseline)	$O(2^{80})$	3DES
标准(standard)	$O(2^{128})$	AES-128,SHA-256
较高(high)	$O(2^{192})$	AES-192,SHA-384
超高(ultra)	$O(2^{256})$	AES-256,SHA-512

7.1.2 对称加密算法

对称加密算法是应用较早的加密算法,技术成熟。在对称加密算法中,数据发信方将明文(原始数据)和加密密钥一起经过特殊加密算法处理后,使其变成复杂的加密密文发送出去。收信方收到密文后,若想解读原文,则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密,才能使其恢复成可读明文。在对称加密算法中,使用的密钥只有一个,发、收信双方都使用这个密钥对数据进行加密和解密,这就要求解密方事先必须知道加密密钥。

对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。不足之处是交易双方都使用同样的密钥,安全性得不到保证。此外,每对用户每次使用对称加密算法时,都需要使用其他人不知道的唯一密钥,这会使得发、收信双方所拥有的钥匙数量呈几何级数增长,密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难,主要是因为密钥管理困难,使用成本较高。在计算机专网系统中广泛使用的对称加密算法有DES、3DES、AES和IDEA等。美国国家标准局倡导的AES已作为新标准取代DES。

对称密码系统的安全性依赖于两个因素:第一,加密算法必须是足够强的,仅仅基于本身去解密信息在实践上是不可行的;第二,加密方法的安全性依赖于密钥的秘密性。因此,没有必要确保算法的秘密性,而需要保证密钥的秘密性。对称加密系统最大的问题是密钥的分发和管理非常复杂,代价高昂。在用户群不是很大的情况下,对称加密系统是有效的,但是对于大型网络,当用户群很大、分布很广时,密钥的分配和保存就成了大问题。对称加密算法的另一个缺点是不能实现数字签名。

7.1.3 非对称加密算法

非对称加密算法又叫公开密钥算法(public key algorithm)。非对称加密算法使用完全

不同但又完全匹配的一对密钥，即公钥和私钥。在使用非对称加密算法加密文件时，只有使用匹配的一对公钥和私钥，才能完成对明文的加密和解密过程。加密明文时采用公钥加密，解密密文时使用私钥才能完成，而且发信方（加密者）知道收信方的公钥，只有收信方（解密者）才是唯一知道自己私钥的人。

非对称加密算法的基本原理是：如果发信方想发送只有收信方才能解读的加密信息，发信方必须首先知道收信方的公钥，然后利用收信方的公钥来加密原文；收信方收到加密密文后，使用自己的私钥才能解密密文。显然，采用非对称加密算法，收、发信双方在通信之前，收信方必须将自己早已随机生成的公钥送给发信方，而自己保留私钥。由于非对称算法拥有两个密钥，因而特别适用于分布式系统中的数据加密。广泛应用的非对称加密算法是 RSA 算法和美国国家标准局提出的 DSA 以及 ECC、DH 等算法。

表 7-2 给出了常用非对称加密算法的安全性对比。可以看出，ECC 算法抗攻击能力强、计算量小、处理速度快、存储空间小、带宽要求低，这使得 ECC 在无线通信安全、IC 卡数据加密等领域广泛应用。然而，由于非对称算法本身的复杂性，使得其对大数据加解密的适用性不强，所以非对称算法常与对称加密算法结合使用，即利用非对称算法对对称算法的密钥进行加密传输。

表 7-2　非对称加密算法安全性对比

攻破时间/MIPS 年	密钥长度/位		密钥长度比
	RSA、DSA	ECC	RSA/ECC
10^4	512	106	5∶1
10^8	768	132	6∶1
10^{11}	1024	160	7∶1
10^{20}	2048	210	10∶1
10^{78}	21 000	600	35∶1

注：1MIPS 年是 1MIPS 的机器一年所能处理的数据量，如表中的 10 000MIPS 年，即表示处理速度为 10 000MIPS 的 CPU 需要 1 年才能攻破。

7.1.4　不可逆加密算法

不可逆加密算法的特征是加密过程中不需要使用密钥，输入明文后由系统直接经过加密算法处理成密文，这种加密后的数据是无法被解密的，只有重新输入明文，并再次经过同样不可逆的加密算法处理，得到相同的加密密文并被系统重新识别后才能真正解密。显然，在这类加密过程中，加密是自己，解密还是自己，而所谓解密，实际上就是重新加一次密，所应用的“密码”也就是输入的明文。不可逆加密算法不存在密钥保管和分发问题，非常适合在分布式网络系统上使用，但因加密计算复杂、工作量相当繁重，通常只在数据量有限的情形下使用，如广泛应用在计算机系统中的口令加密，利用的就是不可逆加密算法。近年来，随着计算机系统性能的不断提高，不可逆加密的应用领域正在逐渐增大。在计算机网络中应用较多不可逆加密算法的有 RSA 公司发明的 MD5 算法和由美国国家标准局建议的不可逆加密标准 SHS(Secure Hash Standard，安全散列标准)等。

7.2 安全协议

安全协议是以密码学为基础的消息交换协议，其目的是在网络环境中提供各种安全服务。密码学是网络安全的基础，但网络安全不能单纯依靠安全的密码算法。安全协议是网络安全的一个重要组成部分。网络安全需要通过安全协议进行实体之间的认证、在实体之间安全地分配密钥或其他各种秘密、确认发送和接收的消息的非否认性等。

下面介绍各类有代表性的安全性协议，它们的目的是保护网络各层的安全，并提供实现保密、认证和完整性的方法。

7.2.1 安全套接层协议

安全套接层(Secure Socket Layer，SSL)协议是由 Netscape 公司设计的一种开放协议。它指定了一种在应用程序协议(例如 HTTP、Telnet、NNTP 或 FIP 和 TCP/IP)之间提供数据安全性分层的机制。它是在传输通信协议(TCP/IP)上实现的一种安全协议，采用公开密钥技术。它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。

SSL 由两层组成：一层是 SSL 记录层，用于封装不同的上层协议；另一层是被封装的协议，即 SSL 握手协议，它可以让服务器和客户机在传输应用数据之前协商加密算法和加密密钥。客户机提出自己能够支持的全部加密算法，服务器可选择最适合它的算法。

SSL 协议通过在应用程序进行数据交换之前交换 SSL 初始握手信息来实现有关安全性的审查。在 SSL 握手信息中，采用了 DES、MD5 等加密技术来实现机密性和数据完整性，并采用 X.509 数字证书实现认证。数字证书是用于验证信息传输出各方身份的有效证明，同时也用于加密数据，防止抵赖和篡改。它通过证书验证和授权机构将证书持有人及其公开密钥的签名有效地关联。

SSL 协议的目标是提供两个应用程序间的通信保密性、可靠性。为了验证数字证书持有者是否是合法的用户，SSL 要求数字证书持有者在握手时交换数据，进行数字式标识。数字证书持有者对包括证书的所有信息进行标识，以说明自己是证书的合法拥有者，防止其他用户冒名使用证书。

SSL 协议提供了 3 种标准服务，即信息保密、信息完整性和双向认证。SSL 协议提供的 3 种标准服务如表 7-3 所示。

表 7-3 SSL 协议提供的 3 种标准服务

安全服务	主要技术	作用
信息保密	加密	防止窃听
信息完整性	信息认证编码	防止破坏
双向验证	X. 509	防止欺骗

1. 信息保密

通过使用公开密钥和对称密钥技术达到信息保密。对称密钥算法的速度要比公开密钥算法的速度快。在 SSL 协议中利用了这两种加密算法，既提供了保密性，又提高了通信效

率。发送方执行的步骤如下。

(1) 产生一个随机数作为对称密钥,接着用它对待发送的明文信息进行加密。

(2) 用接收方的公开密钥对该随机数进行加密。

(3) 用自己的私有密钥对随机数进行解密。

(4) 再用随机数对信息进行解密。

SSL 客户机和 SSL 服务器之间的所有业务,均使用在握手过程中建立的密钥和算法进行加密。这样,就可以防止某些用户通过使用 Sniffer 工具进行非法窃听。

2. 信息完整性

SSL 协议利用机密共享和散列函数组提供信息完整性服务。

3. 双向认证

客户机与服务器相互识别,它们的标识号用公开密钥编码,并在 SSL 握手时交换各自的标识号。

7.2.2　传输层安全协议

传输层安全(Transport Layer Security,TLS)协议是 Internet 工程特别任务组(Internet Engineering Task Force,IETF)定义的一种新的协议。它建立在 Netscape 所提出的 SSL 3.0 协议规范基础之上,是 SSL 3.0 协议的后续版本。在传输层上,TLS 协议在源和目的实体间建立了一条安全通道,提供基于证书的认证、信息完整性和数据保密性。对于用于传输层安全性的标准协议,整个行业好像都正在朝着 TLS 协议的方向发展。在 TLS 协议和 SSL 3.0 协议之间存在着显著的差别(主要是它们所支持的加密算法不同),所以 TLS 1.0 协议和 SSL 3.0 协议不能互操作。

TLS 协议由两层组成:TLS 记录(TLS Record)协议和 TLS 握手(TLS Handshake)协议。较低的层为 TLS 记录协议,位于某个可靠的传输协议(如 TCP)上面。

TLS 记录协议是一种分层协议。每一层中的信息可能包含长度、描述和内容等字段。TLS 记录协议支持信息传输、将数据分段到可处理块、压缩数据、应用 MAC、加密以及传输结果等,对接收到的数据进行解密、校验、解压缩、重组等,然后将它们传送到高层客户机。

TLS 记录协议提供的连接安全性具有两个基本特性。

(1) 私有。对称加密用以数据加密(DES、RC4 等)。对称加密所产生的密钥对每个连接都是唯一的,且此密钥基于另一个协议(如握手协议)协商。TLS 记录协议也可以不加密使用。

(2) 可靠。信息传输包括使用密钥的 MAC 进行信息完整性检查。安全散列功能(SHA、MD5 等)用于 MAC 计算。TLS 记录协议在没有 MAC 的情况下也能操作,但一般只能用于这种模式,即有另一个协议正在使用记录协议传输协商安全参数。

TLS 握手协议由 3 个子协议组构成,允许服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此之间相互认证,协商加密算法和加密密钥。TLS 握手协议提供的连接安全具有以下 3 个基本属性。

(1) 可以使用非对称的或共享密钥密码技术来认证对方的身份。该认证是可选的,但至少需要一个结点方。

(2) 共享加密密钥的协商是安全的。对偷窃者来说协商加密是难以获得的。此外,经过认证过的连接不能获得加密,即使是进入连接中间的攻击者也不能。

(3) 协商是可靠的。没有经过通信方成员的检测,任何攻击者都不能修改通信协商。

TLS 的最大优势就在于 TLS 是独立于应用协议的。高层协议可以透明地分布在 TLS 协议上面。然而,TLS 标准并没有规定应用程序如何在 TLS 上增加安全性;它把如何启动 TLS 握手协议以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

7.2.3 IPSec 协议

IPSec 协议是 IETF 于 1998 年 11 月公布的 IP 安全标准,其目标是为 IPv4 和 IPv6 提供具有较强互操作能力、高质量和基于密码的安全。

IPSec 协议不是一个单独的协议,它给出了应用于 IP 层上网络数据安全的一整套体系结构,包括验证报头(Authentication Header,AH)协议、封装安全载荷(Encapsulating Security Payload,ESP)协议、因特网密钥交换(Internet Key Exchange,IKE)协议和用于网络认证及加密的一些算法等。IPSec 协议提供了访问控制、无连接完整性、数据源鉴别、载荷机密性和有限流量机密等安全服务,弥补了由于 TCP/IP 体系自身带来的安全漏洞。

IPSec 协议规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换,向上层提供了访问控制、数据源认证、数据加密等网络安全服务。

IPSec 协议具有如下优点。

(1) 过滤每一个访问计算机的数据包,并可根据数据包的源 IP 地址、协议和端口进行过滤。

(2) 对应用程序完全透明,应用程序无须任何调整。

(3) 提供 3 种身份验证机制。

(4) 对数据包进行加密,以防止数据包在网络传输中被截取。

(5) 使用散列算法保障数据包在传输过程中保持完整性。

(6) 确保每个 IP 数据包的唯一性。

AH 协议用来进行数据包认证,也就是将每个数据包中的数据和一个变化的数字签名结合起来,使得通信一方确认发送数据的另一方的身份,并且确认数据在传输过程中没有被篡改过。AH 协议可以证明数据的起源地、保障数据的完整性以及防止相同数据包的不断重播。

ESP 协议用来进行数据包加密或认证。使用硬件对数据包中的数据(包括敏感的 IP 地址)进行加密,像 Sniffer 这样的网络监听软件都无法得到任何有用的信息。ESP 协议除了具有 AH 协议的所有功能之外,还可选择保障数据的机密性,以及为数据流提供有限的机密性保障。

安全关联(Security Association,SA)协议定义了在管理两个结点之间的安全通信时使用的安全策略。安全关联在双方能够交换经过认证和加密的安全数据之前,需要就使用哪些算法、如何进行密钥交换、密钥需要多长时间进行更改以及如何真正地交换密钥来达成协议。所有这些值都包含在 SA 中,以便在两个结点之间进行安全通信。

要成功地部署 IPSec,一个可伸缩的、自动的 SA 和密钥管理方案是必不可少的。已经

有多种协议针对这些功能进行了定义。如 ISAKMP(因特网安全与密钥管理协议)定义了 VPN 客户及服务器如何建立关联的框架,使用 ISAKMP,双方可以协商采用哪种加密算法、散列算法、认证机制和密钥建立机制来实现 IPSec 服务;OAKLEY 技术使用 DH 作为协商共享值时的基本机制,但增加了地址验证和认证;因特网密钥交换(Internet Key Exchange,IKE)协议是一种功能强大的、灵活的协商协议,使得 VPN 结点之间达成安全通信的协定,如认证方法、加密方法、所用的密钥、密钥的使用期限,并允许智能的安全密钥交换。

在一个实现 IPSec 的产品中,IPSec 功能的正确性完全依靠安全策略的正确制定与配置。传统的方法是通过手工配置 IPSec 策略,这种方法在大型的分布式网络中存在效率低、易出错等缺点。而一个易出错的策略将可能导致通信的阻塞和严重的安全隐患,而且即使每个安全域策略的制定是正确的,也可能会在不同的安全域中,由于策略之间的交互,出现在局部范围内安全策略的多样性,从而造成端到端间通信的严重安全隐患。因此,必须构建一个安全策略系统来系统地管理和验证各种 IPSec 策略。

IPSec 策略由安全策略数据库(Security Policy Database,SPD)加以维护。在 SPD 中,每个条目都定义了要保护的是什么通信、怎样保护它,以及和谁共享这种保护。对于进入或离开 IP 堆栈的每个包,都必须检索 SPD,调查可能的安全应用。

对一个 SPD 条目来说,它可能定义了下述几种行为:丢弃、绕过以及应用。其中,丢弃表示不让这个包进入或外出;绕过表示不对一个外出的包应用安全服务,也不指望对一个已进入的包进行了保密处理;应用是指对外出的包应用安全服务,同时要求对进入的包已应用了安全服务。对那些定义了应用行为的 SPD 条目,它们均会指向一个或一套 SA,表示要将其应用于数据包。

策略系统的实现也是 IPSec VPN 网关的重要组成部分。只有基于策略的网络系统,才能提供强大的安全机制,才能对网络内部的所有资源提供不同级别的保护。

IPSec 的基本架构定义了用户能以多大的精度来设定自己的安全策略。这样一来,某些通信便可大而化之,为其设置某一级的基本安全措施;而对其他通信则可谨慎对待,为其应用完全不同的安全级别。举个例子,可在一个网络安全网关上制定 IPSec 策略,对在其本地保护的子网与远程网关的子网间通信的所有数据,全部采用 DES 加密,并用 HMAC-MD5 进行验证;另外,从远程子网发给一个邮件服务器的所有 Telnet 数据均用 3DES 进行加密,同时用 HMAC-SHA 进行验证;最后对于需要加密的、发给另一个服务器的所有 Web 通信数据,则用 IDEA 满足其加密要求,同时用 HMAC-RIPEMD 进行验证。

网络攻击者要破译经过 IPSec 加密的数据,即使不是完全不可能,也是非常困难的。根据不同类别数据对于保密需求的不同,IPSec 策略中有多种等级的安全强度可供选择。使用 IPSec 可以显著地减少或防范几种网络攻击。

(1) Sniffer。Sniffer 可以读取数据包中的任何信息,因此对抗 Sniffer,最有效的方法就是对数据进行加密。IPSec 的 ESP 协议通过对 IP 包进行加密来保证数据的私密性。

(2) 数据篡改。IPSec 用密钥为每个 IP 包生成一个数字检查和,该密钥为且仅为数据的发送方和接收方共享。对数据包的任何篡改,都会改变检查和,从而可以让接收方得知包在传输过程中遭到了修改。

(3) 身份欺骗、盗用口令、应用层攻击。IPSec 的身份交换和认证机制不会暴露任何信

息,不给攻击者有可乘之机,双向认证在通信系统之间建立信任关系,只有可信赖的系统才能彼此通信。

(4) 中间人攻击。IPSec 结合双向认证和共享密钥,足以抵御中间人攻击。

(5) 拒绝服务攻击。IPSec 使用 IP 包过滤法,依据 IP 地址范围、协议甚至特定的协议端口号来决定哪些数据流需要受到保护,哪些数据流可以被允许通过,哪些需要拦截。

总之,IPSec 协议族提供了位于网络层的、端到端的传送安全保证。它通过两个基本协议实现,其中由 AH 提供源地址验证和数据完整性检验,但不保证数据隐秘性;而 ESP 协议则提供了数据加密、主机验证和数据完整性检验,可以用来保证数据的隐秘性。除此之外,协议族中的 IKE 协议实现了端到端的自动密钥交换机制。

7.3 网络安全

7.3.1 计算机网络面临的威胁

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭受破坏、更改、泄露,系统连续、可靠、正常地运行,网络服务不中断。

计算机网络所面临的威胁大体可分为两种:一是对网络中信息的威胁;二是对网络中设备的威胁。影响计算机网络的因素很多,有些因素可能是有意的,也可能是无意的;可能是人为的,也可能是非人为的;可能是外来黑客对网络系统资源的非法使用。归纳起来,针对网络安全的威胁主要有如下几种:

(1) 人为的无意失误。如操作员安全配置不当造成的安全漏洞,用户安全意识不强,用户口令选择不慎,用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁。

(2) 人为的恶意攻击。这是计算机网络所面临的最大威胁,敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种:一种是主动攻击,它以各种方式有选择地破坏信息的有效性和完整性;另一种是被动攻击,它是在不影响网络正常工作的情况下进行截获、窃取、破译,以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害,并导致机密数据的泄露。

(3) 网络软件的漏洞和"后门"。网络软件不可能是百分之百的无缺陷和无漏洞。然而,这些漏洞和缺陷恰恰是黑客进行攻击的首选目标,曾经出现过的黑客攻入网络内部的事件,这些事件大部分就是因为安全措施不完善所招致的苦果。另外,软件的"后门"都是软件公司的设计编程人员为了自便而设置的,一般不为外人所知,而一旦"后门"洞开,其造成的后果将不堪设想。

7.3.2 网络安全策略

1. 物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击;验证用户的身份和使用权限、防止用户越权操作;确保计算机系统有一个良好的电磁兼容工作环境;建立完备的安全管理制度,防止非法进入计

算机控制室和各种偷窃、破坏活动的发生。

抑制和防止电磁泄漏是物理安全策略的一个主要问题。目前主要防护措施有两类。一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护，这类防护措施又可分为以下两种：一种是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；另一种是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

2. 访问控制策略

访问控制策略是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问，是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制是保证网络安全最重要的核心策略之一。下面简单介绍各种访问控制策略。

1）入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许用户在哪台工作站入网。

用户的入网访问控制可分为 3 个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查。3 道关卡中只要任何一关未过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法，如果验证合法，才继续验证用户输入的口令，否则，用户将被拒之网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合。用户口令必须经过加密。加密的方法很多，其中最常见的方法有基于单向函数的口令加密、基于测试模式的口令加密、基于公钥加密方案的口令加密、基于二次方剩余的口令加密、基于多项式共享的口令加密、基于数字签名方案的口令加密等。经过上述方法加密的口令，即使是系统管理员也难以得到它。用户也可采用一次性用户口令，还可用便携式验证器（如智能卡）来验证用户的身份。

网络管理员应该可以控制和限制普通用户的账号使用，访问网络的时间、方式。用户名或用户账号是所有计算机系统中最基本的安全形式。用户账号应只有系统管理员才能建立。用户口令应是每个用户访问网络所必须提交的“证件”，用户可以修改自己的口令，但系统管理员应该可以控制口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后，再进一步履行用户账号的默认限制检查。网络应能控制用户登录入网的站点，限制用户入网的时间，限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应能对用户的账号加以限制，用户此时应无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

2）网络的权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋

予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源,可以指定用户对这些文件、目录、设备能够执行哪些操作。可以根据访问权限将用户分为以下几类。

(1) 特殊用户(即系统管理员)。

(2) 一般用户,系统管理员根据用户的实际需要为其分配操作权限。

(3) 审计用户,负责网络的安全控制与资源使用情况的审计。

用户对网络资源的访问权限可以用一个访问控制表来描述。

3) 目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效,用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有8种:系统管理员权限(supervisor)、读权限(read)、写权限(write)、创建权限(create)、删除权限(erase)、修改权限(modify)、文件查找权限(file scan)、存取控制权限(access control)。一个网络系统管理员应当为用户指定适当的访问权限,这些访问权限控制着用户对服务器的访问。8种访问权限的有效组合可以让用户有效地完成工作,同时又能控制用户对服务器资源的访问,从而加强了网络和服务器的安全性。

4) 属性安全控制

当使用文件、目录和网络设备时,网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表,用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限:向某个文件写数据、复制一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件,防止用户对目录和文件的误删除、执行修改、显示等。

5) 网络服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块,可以安装和删除软件等操作。网络服务器的安全控制包括可以设置口令锁定服务器控制台,以防止非法用户修改、删除重要信息或破坏数据;可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

6) 网络监测和锁定控制

网络管理员应对网络实施监控,服务器应记录用户对网络资源的访问和对非法的网络访问,服务器应以图形、文字或声音等形式报警,以引起网络管理员的注意。如果不法之徒企图进入网络,网络服务器应会自动记录企图尝试进入网络的次数,如果非法访问的次数达到设定数值,那么该账户将被自动锁定。

7) 网络端口和结点的安全控制

网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护,并以加密的形式来识别结点的身份。自动回呼设备用于防止假冒合法用户,静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制,用户必须携带证实身份的验证器(如智能卡、磁卡、安全密码发生器)。在对用户的身份进行验证之

后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

8）防火墙控制

这里将防火墙定义为连接两个网络的计算机：一个连接来自受保护的网络；另一个连接通向开放的网络。在 VPN 技术中，受保护的网络称为专用网络，而开放的网络称为公用网络。

防火墙的作用是挡住不需要的 TCP/IP 数据报，让需要的 TCP/IP 数据报通过。有些不需要的数据报可能是假的，黑客发送它们来攻击系统。防火墙的工作就是判定哪个端口正被应用程序使用，有选择地拒绝不允许的所有端口。

通常配置此设备允许信息自由地从企业网（专用网）流向 Internet（公用网），而限制信息从因特网流向企业网。换句话说，任何信息都可以流出，但只有许可的信息才能流入。选择允许通过防火墙的特定 TCP/IP 数据报的过程一般称为过滤。

一种情况是在安装防火墙时，过滤器用来阻塞所有的 TCP/IP 数据报。当然，这样具有立即完全关闭因特网访问的效果。网络管理员这时启用网络操作需要的那些 TCP/IP，这种防火墙允许网络管理员跟踪可以通过和不可以通过的信息。

在第二种情况下，防火墙起初对因特网任一方向的通信几乎没有什么影响。网络管理员必须专门启用过滤器来阻塞所需的端口。只有这些专门启用的过滤器才能影响因特网的访问。这种防火墙的基本想法是对用户尽量少限制，同时又对因特网访问保持某种程度的控制。缺点是管理员很容易错过一两个端口，或错过某个范围的端口，使攻击者有机可乘。

3. 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端-端加密和结点加密 3 种。链路加密的目的是保护网络结点之间的链路信息安全；端-端加密的目的是对源端用户到目的端用户的数据提供保护；结点加密的目的是对源结点到目的结点之间的传输链路提供保护。用户可根据网络情况酌情选择加密方式。

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是应对恶意软件的有效方法之一。

4. 网络安全管理策略

在网络安全中，除了采用上述技术措施之外，加强网络的安全管理、制定有关规章制度，对于确保网络安全和可靠运行，将起到十分有效的作用。

网络的安全管理策略包括：确定安全管理等级和安全管理范围；制定有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。

7.4 系统安全

7.4.1 操作系统安全

1. 安全操作系统

操作系统是应用软件同系统硬件的接口。在信息系统安全涉及的众多内容中，操作系统、网络系统与数据库管理系统的安全问题是核心。没有系统的安全就没有信息的安全。

作为系统软件中最基础部分的操作系统，其安全问题的解决又是关键中之关键。

安全操作系统(secure operating system)指的是能对所管理的数据与资源提供适当的保护级、有效地控制硬件与软件功能的操作系统。若没有安全操作系统的支持，数据库就不可能具有存取控制的安全可信性，就不可能有网络系统的安全性，也不可能有应用软件信息处理的安全性。因此，安全操作系统是整个信息系统安全的基础。

就安全操作系统的形成方式而言，一种是从系统开始设计时就充分考虑到系统的安全性的安全设计方式，另一种是基于一个通用的操作系统，专门进行安全性改进或增强的安全增强方式。安全操作系统在开发完成后，在正式投入使用之前一般都要求通过相应的安全性评测。

对操作系统安全的威胁主要有以下几方面。

(1) 以操作系统为手段，获得授权以外或未授权的信息。它危害计算机及其信息系统的机密性和完整性。

(2) 以操作系统为手段，阻碍计算机系统的正常运行或用户的正常使用。它破坏计算机系统的完整性，危害了计算机系统的可用性。

(3) 以软件为对象，非法复制和非法使用。

(4) 以操作系统为手段，破坏计算机及其信息系统的安全，窃取或非法获取系统的信息。

操作系统的安全性对计算机系统和信息系统的安全性有着至关重要的影响。目前，大多计算机攻击都利用了操作系统和系统应用程序的安全漏洞，即操作系统存在的安全缺陷。工业界已经承认这样一个事实：任何操作系统都是有缺陷的，但绝大多数操作系统是可靠的，可以基本完成其设计功能。操作系统的设计必须解决以下两个相互抵触的要求。

(1) 用户应能使用(调用)操作系统。

(2) 用户不能滥用操作系统。

操作系统安全的主要目标如下。

(1) 标识系统中的用户，并进行身份鉴别。

(2) 依据系统安全策略对用户的操作进行访问控制，防止用户对计算机资源的非法访问(窃取、篡改和破坏)。

(3) 监督系统运行的安全性。

(4) 保证系统自身的安全性和完整性。

从用户观点，要求操作系统提供的基本的安全服务有如下几方面。

(1) 存储保护。

(2) 文件保护。

(3) 一般客体的访问控制(general object access control)。

(4) 用户鉴别。

如果操作系统有以一致的且有效的方式提供上述4个服务的置信度，则称该操作系统是可信的。也可以说，可信操作系统是一个使用了足够的硬件和软件完整性机制，能够用来同时处理大量敏感或分类信息的系统。可信操作系统涉及下列关键概念。

(1) kernelized design(内核化设计)。

(2) security kernel(安全内核)。

（3）reference monitor（基准监视器）。

（4）trusted computing base（TCB，可信计算基）。

（5）virtualization（虚拟化）。

（6）layered design（分层设计）。

从设计者的观点，根据提供安全服务的构件的设计和功能来查看可信操作系统。可信操作系统的 4 个主要基础如下。

（1）安全策略。安全策略定义了一组意义明确的、一致的和可实现的规则，而且这些规则能被非常清楚地、无二义地表达处理，满足操作系统的安全需求。

（2）模型。用形式化的方法来描述如何实现系统的机密性、完整性和可用性等安全需求，模型是策略的一种表示。

（3）设计。设计包括可信操作系统是什么、它期望的功能以及它是如何构造的，即它的实现。

（4）信任。对一个系统的信任基于两方面：一方面是特征，即操作系统包含了实施安全策略所必需的所有功能；另一方面是保证，即操作系统的实现方式使人们信任它能够正确且有效地实施安全策略。

2. 安全操作系统等级划分

对安全操作系统的研究，始于美国国防部 1967 年启动的安全操作系统项目 Adept-50，经历了奠基时期、多策略时期和动态策略时期。国内安全操作系统研究起步较晚，但目前已被广泛重视，国内军用安全操作系统的研究还处于起步阶段。而美军早在 20 世纪 80 年代已开始有了 B2 级以上的高安全等级操作系统，但对我国进行技术封锁。

国际上计算机系统安全研究影响重大的一个显著成果是安全产品的评价标准。美国国防部于 1983 年提出并于 1985 年批准的可信计算机系统安全评价准则（TCSEC）（又称“橘皮书”）为计算机安全产品的评测提供了测试准则和方法，指导信息安全产品的制造和应用，并建立了关于网络系统、数据库等的安全解释。TCSEC 将计算机系统的安全可信性分为 4 等 8 个级别。安全等级按 D、C1、C2、B1、B2、B3、A1、超 A1 渐次增强，如表 7-4 所示。

表 7-4　TCSEC 的安全分级表

级　别	名　　称	主 要 特 征
超 A1	可信任分布级	硬件和软件在物理传输过程中已经受到保护，以防止破坏安全系统
A1	验证设计级	形式化验证安全模型，形式化隐蔽通道分析
B3	安全域防护级	安全内核，高抗渗透能力
B2	结构化防护级	形式化安全模型，隐秘通道约束，面向安全的体系结构，较好的抗渗透能力
B1	符号安全防护级	强制访问控制，安全标识，删去与安全相关的缺陷
C2	受控访问防护级	受控自主访问控制，增加审核机制，记录安全性事件
C1	选择性安全防护级	要求硬件有一定的安全防护
D	最低防护级	最低等级

D 级是最低的安全级别，整个计算机系统是不可信任的。硬件和操作系统很容易被侵袭。任何人都可以自由地使用该计算机系统，不对用户进行验证。系统不要求用户进行登

记(要求用户提供用户名)或使用密码(要求用户提供唯一的字符串来进行访问)。任何人都可以坐在计算机的旁边并使用它。DOS、Windows 3.x 及 Windows 95(不在工作组方式中)都属于D级的计算机操作系统。

C级分为C1级和C2级。C1级是选择性安全防护(discretionary security protection)系统,要求硬件有一定的安全保护(如硬件有带锁装置,需要钥匙才能使用计算机)。用户在使用计算机系统前必须先登录。另外,作为C1级保护的一部分,允许系统管理员为一些程序或数据设立访问许可权限。UNIX系统、Novell 3.x或更高版本、Windows NT都属于C1级兼容计算机操作系统。C2级引进了受控访问环境(用户权限级别)的增强特性,具有进一步限制用户执行某些命令或访问某些文件的权限,而且还加入了身份认证级别。能够达到C2级的常见操作系统有UNIX、Novell 3.x或更高版本、Windows NT。

B级分为B1、B2和B3共3个子级。B1级:指符号安全防护(label security protection),支持多级安全。"符号"是指网上的一个对象,该对象在安全防护计划中是可识别且受保护的。"多级"是指这一安全防护安装在不同级别,对敏感信息提供更高级的保护,让每个对象都有一个敏感标签,而每个用户都有一个许可级别。B1级安全措施的计算机系统随着计算机系统而定,政府机构和防御承包商们是B1级计算机系统的主要拥有者。B2级又称为结构化防护(structured protection),要求计算机系统中所有对象加标签,而且给设备(如工作站、终端和磁盘驱动器)分配安全级别。如允许用户访问一台工作站,但不允许访问含有职员工资资料的磁盘子系统。B3级又称为安全域(security domain),要求用户工作站或终端通过可信任途径连接网络系统,而且这一级采用硬件来保护安全系统的存储区。

A级是橘皮书中的最高安全级,又称为验证设计(verity design),它包括了一个严格的设计、控制和验证过程。与前面所提到的各级别一样,该级别包含了较低级别的所有特性。设计必须是从数学角度经过验证的,而且必须进行秘密通道和可信任分布的分析。可信任分布(trusted distribution)的含义是,硬件和软件在物理传输过程中已经受到保护,以防止破坏安全系统。

安全操作系统通常与相应的安全等级相对应,例如,根据TCSEC标准,通常称B1级以上的操作系统为安全操作系统。

3. 普通操作系统与可信操作系统在安全特性方面的区别

普通操作系统的安全特性包括用户鉴别、内存保护、文件和输入输出设备访问控制,对一般对象的分配和访问控制,共享的实施,保证公平服务、进程间通信和同步,对操作系统保护数据的保护。

可信操作系统的安全特性包括用户识别和鉴别、强制访问控制、自主访问控制、对象重用保护、完全检查、可信路径(可信通路)、审计、审计日志精简、入侵检测等。

用户身份识别和鉴别是众多计算机安全的基础,它是用户鉴别和用户身份的唯一标识。

强制访问控制指的是访问控制策略的判决不受一个对象的单个拥有者的控制,中央授权系统决定哪些信息可被哪些用户访问,而用户自己不能够改变访问权限。

自主访问控制指的是拥有者能够决定谁应该拥有对其对象的访问权及其内容。在商业环境中,常用自主访问控制来允许指定群体中的所有人(有时是其他的命名个体)改变访问权。强制访问控制和自主访问控制可同时应用于同一个对象。强制访问控制的优先权要高于自主访问控制。

对象重用保护指对曾经包含一个或几个客体的存储介质(如页帧、盘扇面、磁带)重新分配和重用。为了安全地进行重分配、重用,要求介质不得包含重分配前的残留数据。计算机保持其效率的一种方法就是对象重用,但对象重用可能产生严重的脆弱点。通常,文件占用的空间来自于磁盘上先前被用过、但现在已被释放的空间,或其他存储设备上的空间。被释放的空间是"脏"的,也就是说,它仍然包含先前用户的数据。恶意的用户会申请大量磁盘空间,然后从中获取敏感信息。这种攻击被称为对象重用攻击。这个问题包括磁盘、主存、处理器的寄存器、其他磁介质(例如磁带)或者其他可重用的存储媒体。磁介质对于此类攻击尤其脆弱。非常精密和昂贵的仪器有时候能够将最近的数据和它先前记录的数据分开,然后再将后者与后者之前的数据分开,以此类推。这种威胁,称为磁记忆。在任何情况下,操作系统在允许对资源的访问之前必须负责清除资源上的信息。

完全检查指的是所有主体对客体的访问必须受到控制。高可信操作系统执行完全检查,意思就是所有的访问必须经过检查。为了让强制或者自主访问控制有效,所有的访问必须受到控制。如果攻击者通过内存、外部端口、网络或者隐蔽通道请求访问,那么仅仅对文件的访问进行控制是不够的。由于需要控制更多的访问路径,可信操作系统的设计和实现难度就大大增加了。高可信操作系统执行完全检查,意思就是所有的访问必须经过检查。

可信路径是终端人员能借以直接与可信计算机通信的一种机制。该机制只能由有关终端操作人员或可信计算机启动,并且不能被不可信软件模仿。恶意用户获得不合适访问的一种途径就是"欺骗"用户,使用户认为自己正和一个合法的安全系统在通信,而实际上这时候键入的内容以及命令已经被截获且分析了。因此,对于关键的操作,如设置口令或者更改访问许可,用户希望能进行无误的通信(称为可信通路),以确保用户只向合法的接收者提供这些重要的、受保护的信息。

在一些操作系统中,用户通过输入一个唯一的键序列[如 Windows NT 操作系统的 Ctrl+Alt+Del 键,这个唯一的键序列称为安全注意序列(Secure Attention Sequence, SAS)]来请求一条可信通路。这个唯一的键序列在设计上直接被安全实施软件截获。在其他可信系统中,与安全相关的改变只能在系统启动的时候进行。也就是说,改变只能在除安全实施代码外的其他任何进程运行之前进行。

可审计性通常涉及维护与安全相关的、已发生的事件日志,即列出每一个事件和所有执行过添加、删除或改变操作的用户。显然,需要保护审计日志不被外界访问,并且记录所有与安全相关的事件。

与审计日志精简紧密联系的是检测安全漏洞的能力,理想情况下是在它们发生的时候就被检测出来。在审计日志中有太多的信息需要去分析。计算机有助于将独立数据联系起来。入侵检测软件构造了正常系统使用的模式,一旦使用出现异常就发出警告。检测的基本方法有基于日志和基于消息认证码(Message Authentication Code,MAC),主动监视入侵者的异常行为,且能触发报警。

7.4.2　数据库系统安全

1. 数据库安全概述

数据库系统一般可以理解成两部分:一部分是数据库,按一定的方式存取数据;另一部分是数据库管理系统(DBMS),为用户及应用程序提供数据访问,并具有对数据进行维护等

对象重用保护指对曾经包含一个或几个客体的存储介质(如页帧、盘扇面、磁带)重新分配和重用。为了安全地进行重分配、重用,要求介质不得包含重分配前的残留数据。计算机保持其效率的一种方法就是对象重用,但对象重用可能产生严重的脆弱点。通常,文件占用的空间来自于磁盘上先前被用过、但现在已被释放的空间,或其他存储设备上的空间。被释放的空间是“脏”的,也就是说,它仍然包含先前用户的数据。恶意的用户会申请大量磁盘空间,然后从中获取敏感信息。这种攻击被称为对象重用攻击。这个问题包括磁盘、主存、处理器的寄存器、其他磁介质(例如磁带)或者其他可重用的存储媒体。磁介质对于此类攻击尤其脆弱。非常精密和昂贵的仪器有时候能够将最近的数据和它先前记录的数据分开,然后再将后者与后者之前的数据分开,以此类推。这种威胁,称为磁记忆。在任何情况下,操作系统在允许对资源的访问之前必须负责清除资源上的信息。

完全检查指的是所有主体对客体的访问必须受到控制。高可信操作系统执行完全检查,意思就是所有的访问必须经过检查。为了让强制或者自主访问控制有效,所有的访问必须受到控制。如果攻击者通过内存、外部端口、网络或者隐蔽通道请求访问,那么仅仅对文件的访问进行控制是不够的。由于需要控制更多的访问路径,可信操作系统的设计和实现难度就大大增加了。高可信操作系统执行完全检查,意思就是所有的访问必须经过检查。

可信路径是终端人员能借以直接与可信计算机通信的一种机制。该机制只能由有关终端操作人员或可信计算机启动,并且不能被不可信软件模仿。恶意用户获得不合适访问的一种途径就是“欺骗”用户,使用户认为自己正和一个合法的安全系统在通信,而实际上这时候键入的内容以及命令已经被截获且分析了。因此,对于关键的操作,如设置口令或者更改访问许可,用户希望能进行无误的通信(称为可信通路),以确保用户只向合法的接收者提供这些重要的、受保护的信息。

在一些操作系统中,用户通过输入一个唯一的键序列[如 Windows NT 操作系统的 Ctrl+Alt+Del 键,这个唯一的键序列称为安全注意序列(Secure Attention Sequence,SAS)]来请求一条可信通路。这个唯一的键序列在设计上直接被安全实施软件截获。在其他可信系统中,与安全相关的改变只能在系统启动的时候进行。也就是说,改变只能在除安全实施代码外的其他任何进程运行之前进行。

可审计性通常涉及维护与安全相关的、已发生的事件日志,即列出每一个事件和所有执行过添加、删除或改变操作的用户。显然,需要保护审计日志不被外界访问,并且记录所有与安全相关的事件。

与审计日志精简紧密联系的是检测安全漏洞的能力,理想情况下是在它们发生的时候就被检测出来。在审计日志中有太多的信息需要去分析。计算机有助于将独立数据联系起来。入侵检测软件构造了正常系统使用的模式,一旦使用出现异常就发出警告。检测的基本方法有基于日志和基于消息认证码(Message Authentication Code,MAC),主动监视入侵者的异常行为,且能触发报警。

7.4.2　数据库系统安全

1. 数据库安全概述

数据库系统一般可以理解成两部分:一部分是数据库,按一定的方式存取数据;另一部分是数据库管理系统(DBMS),为用户及应用程序提供数据访问,并具有对数据进行维护等

冗余度小,修改的数据几乎无法恢复。因此必须有一套数据库恢复技术,以保证在系统或程序出现故障后,帮助恢复数据库。当多个用户同时向数据库进行存取操作时,也可能会破坏数据的完整性。

2）数据库面临的安全威胁

凡是造成对数据库内存储数据(包括敏感、非敏感的信息)的非授权的访问(如读取)或非授权的写入(如增加、删除、修改等),原则上都属于对数据库的数据安全造成了威胁或破坏。另外,凡是正常业务需要访问数据库时,令授权用户不能正常得到数据库的数据服务时,也认为对数据库的安全形成了威胁或破坏。因为这两种情况都会对数据库合法用户的权益造成侵犯,或者是信息的被窃取,或者是由于信息的破坏而形成提供错误信息的服务,或者是干脆拒绝提供服务。

对数据库安全的威胁或侵犯大致可以分为以下几类。

(1）偶然的、无意的侵犯或破坏。自然的或意外的事故,例如地震、水灾和火灾等导致的硬件损坏,进而导致数据的损坏和丢失。

(2）硬件、软件故障或错误导致的数据丢失。硬件、软件故障或错误可能导致系统内部的安全机制的失效,也可能导致非法访问数据或系统拒绝提供数据服务。

(3）人为的失误。操作人员或者系统的直接用户的错误输入或对应用系统的不正确使用。

(4）蓄意的侵犯或敌意的攻击。授权用户可能滥用其权限,蓄意窃取或破坏信息。

(5）病毒。病毒可以自我复制,永久地或通常是不可恢复地破坏自我复制的现场,达到破坏信息系统、取得信息甚至使对方丧失战斗力的目的。

(6）特洛伊木马。一些隐藏在公开的程序内部收集环境的信息,可能是由授权用户(不经意)安装的,利用用户的合法权限对数据的安全进行攻击。

(7）天窗、隐通道。藏在合法程序内部的一段程序代码,在特定的条件下(例如特殊的一段输入数据)启动,从而许可此时的攻击可以跳过系统设置的安全机制进入系统,以实现对数据防范的攻击和达到窃取数据的目的。

(8）信息的非正常扩散——泄密。

(9）由授权读取的数据,通过推论得到不应访问的数据。

(10）对信息的非正常修改,包括破坏数据一致性的非法修改以及删除。

(11）敌对方的攻击,内部或外部的非授权用户从不同渠道进行攻击。

(12）敌对方对软件或硬件的肆意破坏。

(13）绕过DBMS直接对数据进行读写。

(14）其他。通过各种途径干扰数据库管理系统的正常工作状态,使之在正当用户提出数据请求时,不能随时提供数据服务。

3）数据库的安全需要

面对数据库的安全威胁,必须采取有效的措施,以满足对数据安全的需求。数据的安全可分为逻辑安全与物理安全两类。数据的物理安全是指在不改变应用软件的前提下,改变物理存储特征,例如存储块的大小、存储方法、设备能力等。数据的逻辑安全是指在不改变现有程序的前提下,支持新的应用或现有数据的新应用的能力。对数据库系统的一个重要要求是保障其应用程序的数据独立性,包括逻辑数据独立性和物理数据独立性。

(1) 数据库的安全性要求。

数据库的安全性要求如表 7-5 所示。

表 7-5 数据库的安全性要求

安全性问题	注 释
物理上的数据完整性	预防数据库数据物理方面的问题，如掉线以及当被灾祸破坏后能重构数据库
逻辑上的数据完整性	保持数据的结构，如一个字段的值的修改不至于影响其他字段
元素的完整性	包含在每个元素中的数据是准确的
可审计性	能够追踪到谁访问过或修改过数据库的元素
访问控制	允许用户只访问被批注的数据，以及限制不同的用户有不同的访问模式，如读或写
用户认证	确保每个用户被正确识别，既便于审计追踪，也为了限制对特定的数据进行访问
可获用性	用户一般可以访问数据库以及所有被允许访问的数据

① 数据库完整性。它是数据库管理系统(DBMS)、操作系统(OS)和计算机管理者三方面应负的责任。数据库管理程序必须进行访问控制，确保只有授权用户才能进行数据更新或删除。另外还须防范非人为的外力灾难。从操作系统和计算机管理者的角度看，数据库和 DBMS 分别是文件和程序，要保护数据库的完整性，必须定期地对数据库文件进行备份，以预防因灾难造成的损失。数据库数据的完整性包括物理上和逻辑上的数据完整性两种。

② 元素的完整性。它是指数据库元素的正确性和准确性。DBMS 要能帮助用户发现输入时的错误，并能在输入错误数据后及时纠正它们。DBMS 用 3 种方式维护数据库中每个数据元素的完整性。

- 字段检查。可防止输入数据时可能出现的错误。
- 访问控制。保护数据库的完整性、真实性和一致性。
- 更改日志。根据数据库每次改变的记录文件，包括记录原来的值和修改后的值的文件，数据库管理员可以随时撤销任何错误的和非法的修改。

③ 可审计性。在某些应用中，可能需要产生对数据库的所有访问的审计记录，以帮助在事后发现发生过什么事件、何人参加、有何影响等，以协助维护数据库的完整性。数据库的审计踪迹包括对记录、字段和数据元素一级的访问。

④ 访问控制。DBMS 必须批准哪些数据可以访问，哪些数据禁止访问。其数据可以是字段，也可以是记录，或者是某个数据元素。DBMS 可批准一个用户有权读、改变、删除或附加一个值，还可以增加或删除整个字段或记录，或者重新组织数据库。

⑤ 用户认证。DBMS 应严格进行用户身份识别和认证。DBMS 可能要求用户输入口令和时间日期，以做检查。

⑥ 可获用性。数据库中的数据并不是任何用户都可以访问的。例如，一个用户在更新几个字段时，其他的用户对这几个字段的访问请求便被禁止。当更新完毕时，其他用户对这些字段的访问权即可获得。

表 7-6 列出了数据库的安全功能和安全过程。

表 7-6　数据库的安全功能和安全过程

区　　域	安全功能和安全过程
外部过程	个人安全许可证 口令保护 信息等级和安全策略规划 监测和段落处理
通信线路	数据加密
物理环境	确定文件/处理者/计算机终端的安全区 电磁辐射的屏蔽和防泄漏
数据存储	数据加密 数据备份(复制)
计算机硬软件	用户授权,存取控制,监视记录,数据的痕迹,内容保护,设立特权状态,提高计算机软硬件的可靠性

(2) 数据库的安全需求。

为了维护数据库的安全,客观上需要一个安全的操作系统和一个运行可靠的数据库管理系统。

① 对操作系统的安全需求。

- 应能防止对 DBMS 和用户程序的非法修改。
- 应能保护存储器中的数据不被非法修改。
- 应能保护数据,使其中的数据安全、完整。
- 应能认证数据库的合法用户,当非法用户进入时能及时报警。
- 应能正确地进行物理 I/O 操作。

② 对数据库管理系统的要求。

数据库的安全需要一个可供运行的、可靠的 DBMS,要求如下。

- 有正确的编译功能,能正确地进行规定的操作。
- 能提供正确的系统变量值,正确地执行命令文件。
- 能保证数据的安全性与完整性,能抵御物理破坏(例如因突然断电或其他灾害造成的损失),能维护数据库逻辑的完整性,能恢复数据库中的内容,对数据元素的修改不影响其他数据。
- 能进行用户识别和访问控制,限制用户只能访问被授权的数据,对不同的用户限制在不同的状态下进行访问。
- 用户能顺利地访问数据库中授权的数据和一般的数据,不会出现拒绝服务的情况,并能进行安全的通信。

4) 数据库的安全技术

数据库的安全技术主要有口令保护、数据加密、数据库加密和数据库的访问控制。

(1) 口令保护。口令设置是信息系统的第一道屏障,口令保护尤其重要。对数据库的不同功能块应设置不同的口令,对存取它的用户应设置不同的口令级别。各种模块(如读模块、写模块和修改模块等)之间的口令应彼此独立,并且应将口令进行加密,以保护数据安全。

现在,有一种口令管理方式能在最大程度上确保使用者是合法用户,这种口令管理方称

为零知识证明,简称零式方式。这种方式对一个真正的被授权用户来说,其口令不可能被冒充、复制或破坏。在进行用户身份验证时,不用提供可能为窃听者使用或计算口令所用的任何信息。零式方式的关键是必须有一个绝对可靠的数据库系统安全管理员,当一个用户将进入系统时,安全员需对其身份进行验证。具体的工作步骤如下。

① 用户获取一个随机数,并使其与自己所持的密钥一并处理,将结果传送给数据库安全管理员。

② 数据库安全管理员获取一个随机数,并将此数字传送给用户。

③ 用户将此随机数同自己的密钥一并处理,并将其结果再一次传送给数据库安全管理员。

④ 数据库安全管理员检查这个回答是否正确。若正确,则减少对用户真实身份一半的怀疑;如果不正确,则停止用户的进一步活动。

以上 4 个步骤可连续重复几十次,如 20～30 次,如果每次回答均正确,则数据库安全管理员对用户身份的怀疑可减少到零。这时,该用户便被确认为合法用户。

(2) 数据加密。考虑到用户可能试图旁路系统的情况,如物理地取走数据、在通信线路上窃听,对这样的威胁最有效的解决方法就是数据加密,即以加密格式存储和传输敏感数据。关于数据加密原理、加密算法详见 7.1 节。

(3) 数据库加密。数据库系统担负着存储和管理关键业务数据和信息的任务。如何保证和加强数据库系统的安全性和保密性,是每个信息系统都必须解决的重要课题。一般而言,数据库系统提供的基本安全技术能够满足一般应用的要求。但对于一些重要部门或敏感领域的应用,仅靠上述这些措施是难以充分保证数据的安全性的。

某些用户,尤其是一些内部用户,仍可能非法获取用户名、口令字,或利用其他方法越权使用数据库,甚至可以直接打开数据库文件来窃取或篡改信息。因此,有必要对数据库中存储的重要数据进行加密处理,以强化数据存储的安全保护。

数据库的加密方式很多,既可以软件加密,也可以硬件加密。软件加密可以采用库外加密,也可以采用库内加密。库外加密方式即采用文件加密的方法,它把数据库作为一个文件,把每一个数据块当作文件的一个记录进行加密。文件系统与数据库管理系统交换的就是块号。库内加密按加密的程度,可以进行记录加密,也可以进行字段加密,还可以对数据元素进行加密。数据元素加密时,每个元素被当作一个文件进行加密。硬件加密是在物理存储器(磁盘)与数据库文件之间加一个硬件装置,使之与实际的数据库脱离,加密时只对某一磁盘上的数据加密。

与传统的数据加密技术相比,数据库密码系统有其自身的要求和特点。一般数据库的数据以原始形式存放在数据库内,因此对于计算机专家,特别是数据库厂家和专家或者有意攻击者来说基本上是透明的。只要通过简单分析即可获得数据的本来形式,这是数据库系统的一个严重的不安全因素,即所谓数据以原始形式——可读形式存放在数据库中。不仅是信息泄露问题,而且数据的可信度也成问题,数据的真实性无法核实。除了在数据处理和传输过程中进行访问控制、加密处理之外,最好是对存储在数据库内的数据也进行加密处理,这对于保证数据库数据的保密性和真实性是非常重要的。

(4) 数据库的访问控制。数据库系统可以允许数据库管理员和有特定访问权限的用户有选择地、动态地把访问权授予其他用户;如果需要,也可以收回这些权利。这些权利存在

一张访问控制表中。

当一个新的用户需要访问数据库资源时，首先由数据库管理人员或数据库拥有者对该用户进行注册，给该用户分配一个口令，并授予其访问相应系统资源的权利。然后，由该用户输入注册口令。若口令正确，就可以使用该数据库资源。若未经授权，任何用户都不能使用该数据库资源。

为了增加数据库的安全性，可以随时更改用户的口令。这样，不仅增加了用户的安全感，也增强了系统的保密性。

7.5 应用安全

7.5.1 Web 安全

随着 Web 2.0、社交网络、微博等一系列新型互联网产品的诞生，基于 Web 环境的互联网应用越来越广泛，例如企业在信息化的过程中将各种应用都架设在了 Web 平台上。Web 业务的迅速发展也引起了黑客们的强烈关注，接踵而至的就是 Web 安全威胁的凸显。黑客利用网站操作系统的漏洞和 Web 服务程序的 SQL 注入漏洞等得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。这也使得越来越多的用户关注应用层的安全问题，对 Web 应用安全的关注度也逐渐升温。

下面对一些常见的 Web 应用安全隐患及其防范方法做简单介绍。

1. SQL 注入攻击

SQL 注入(SQL injection)攻击简称注入攻击，是发生于应用程序的数据库层的安全漏洞。简而言之，是在输入的字符串之中注入 SQL 指令，在设计不良的程序当中忽略了检查，那么这些注入进去的指令就会被数据库服务器误认为是正常的 SQL 指令而运行，因此数据库遭到破坏或入侵。

有部分人认为 SQL 注入攻击是只针对 Microsoft SQL Server 而来，但只要是支持批处理 SQL 指令的数据库服务器，都有可能受到此种手法的攻击。

预防方法如下。

(1) 严格限制 Web 应用的数据库的操作权限，给此用户提供仅仅能够满足其工作的最低权限，从而最大限度地减少注入攻击对数据库的危害。

(2) 检查输入的数据是否具有所期望的数据格式，严格限制变量的类型，例如使用 regexp 包进行一些匹配处理，或者使用 strconv 包对字符串转换成其他基本类型的数据进行判断。

(3) 对进入数据库的特殊字符(′、″、\、<、>、&、*、;等)进行转义处理或进行编码转换。

(4) 对所有的查询语句，建议使用数据库提供的参数化查询接口。参数化的语句使用参数而不是将用户输入的变量嵌入到 SQL 语句中，即不要直接拼接 SQL 语句，例如使用

Database/SQL 里面的查询函数 Prepare()和 Query(),或者 Exec(query string, args ... interface{})。

(5) 在应用发布之前建议使用专业的 SQL 注入检测工具进行检测,以及时修补被发现的 SQL 注入漏洞。网上有很多这方面的开源工具,例如 sqlmap、SQLninja 等。

(6) 避免网站打印出 SQL 错误信息,如类型错误、字段不匹配等,把代码里的 SQL 语句暴露出来,以防止攻击者利用这些错误信息进行 SQL 注入。

2. 跨站脚本攻击

跨站脚本(Cross-Site Scripting, XSS[①])攻击是一种网站应用程序的安全漏洞攻击,是代码注入的一种。它允许恶意用户将代码注入网页上,其他用户在观看网页时就会受到影响。这类攻击通常包含了 HTML 以及用户端脚本语言。

XSS 攻击通常指的是通过利用网页开发时留下的漏洞,通过巧妙的方法注入恶意指令代码到网页,使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是 JavaScript,但实际上也可以包括 Java、VBScript、ActiveX、Flash 甚至是普通的 HTML。攻击成功后,攻击者可能得到更高的权限(如执行一些操作)、私密网页内容、会话和 Cookie 等各种内容。

预防方法如下。

(1) 过滤特殊字符。避免 XSS 攻击的方法之一是将用户所提供的内容进行过滤。

(2) 使用 HTTP 头指定类型。使用'w. Header(). Set("Content-Type","text/javascript")',就可以让浏览器解析 JavaScript 代码,而不会是以 HTML 输出。

3. 非法文件上传

MIME 在互联网可以用来标识文件的类型,如.png 文件的 MIME 是 image/png,.php 文件的 MIME 是 text/plain。写过程序的人都知道,自己在上传文件的时候为了安全,通常会使用 MIME 来判定一个文件的类型。

预防方法如下。

(1) 客户端验证。客户端使用 JavaScript 检测,在文件上传时,就对文件进行验证。

(2) 服务器端检测。服务器端脚本一般会检测文件的 MIME 类型、文件扩展名,甚至可以检测文件中是否嵌入恶意代码。

4. 越权访问

越权访问漏洞又可以分为平行越权访问漏洞与垂直越权访问漏洞两类。平行越权访问漏洞指的是权限平级的两个用户之间的越权访问;垂直越权访问漏洞指的是权限不等的两个用户之间的越权访问。

预防方法如下。

(1) 水平权限攻击。从用户的加密认证 Cookie 中获取当前用户 id,并且在执行的 SQL 语句中加入当前用户 id 作为条件语句。由于 Cookie 是加密的,所以攻击者无法修改加密信息。

---

① 跨站脚本为了避免与 CSS 相混淆,所以简称为 XSS。

(2) 垂直权限攻击。在每个页面的加载之前进行权限验证即可。一个普通的权限系统,菜单是通过数据库中对应权限和角色来进行字符串拼接形成的,而不是静态地通过在页面上进行权限判断决定的。

7.5.2　电子邮件安全

随着因特网的发展,电子邮件作为一种通信方式逐渐普及。当前电子邮件的用户已经从科学和教育行业发展到普通家庭中的用户,电子邮件传递的信息也从普通文本信息发展到包含声音、图像在内的多媒体信息。随着用户的增多和使用范围的逐渐扩大,保证邮件本身的安全以及电子邮件对系统安全性的影响越来越重要。

电子邮件在因特网上传输,从一台计算机传输到另一台计算机。在电子邮件所经过的网络上的任一系统管理员或黑客都有可能截获和更改该邮件,甚至伪造某人的电子邮件。与传统邮政系统相比,电子邮件与密封邮寄的信件并不相像,而与明信片更为相似。因此电子邮件本身的安全性是以邮件经过的网络系统的安全性和管理人员的诚实、对信息的漠不关心为基础的。

邮件本身的安全首先要保证邮件不被无关的人窃取或更改,同时接收者也必须能确定该邮件是由合法发送者发出的。针对电子邮件采用的安全技术主要是加密技术,但当前还没有安全电子邮件的正式标准。重要的标准草案有 S/MIME、PGP 和 PEM。

1. S/MIME

S/MIME(Secure/Multipurpose Internet Mail Extension)由 RSA 算法专利的拥有者 RSA 数据安全公司所制定,使用 X509 标准的树状认证结构。这个标准得到了 Microsoft 和 Netscape 等大多数商业公司的支持,并将很快得到 IETF 承认。S/MIME 提供的功能如下。

(1) 封装数据。加密内容和加密密钥。

(2) 签名数据。发送者对消息进行签名,并用私钥加密,对消息和签名都使用 Base64 编码,签名后的消息只有使用 S/MIME 的接收者才能阅读。

(3) 透明签名数据。发送者对消息签名,但只有签名使用 Base64 编码,接收者即使没有使用 S/MIME,也可以阅读消息内容,但不能验证签名。

(4) 签名和封装数据。加密后的数据可以再签名,签名和透明签名过的数据可以再加密。S/MIME 所使用的密码算法有 SHA、MD5、DSS、RSA、Diffie-Hellman、RC2 和 DES 等。

2. PGP

美国人 Phil Zimmermann 提出的 PGP(Pretty Good Privacy)是一种混合密码系统,包含 4 个密码单元,即分组密码(IDEA、CAST、3DES),公开密码(Diffie-Hellman、RSA、DSS),单向散列算法(SHA、MD5)和一个随机数发生算法。可以用 PGP 对邮件保密,以防止非授权者阅读,还能对邮件加上数字签名,从而使收信人可以确信邮件是谁发来的。它让用户可以安全地和从未见过的人通信,事先并不需要任何保密的渠道用来传递密钥。

PGP 的优点在于把 RSA 公钥密码系统的方便和传统密码系统的高速度结合起来,并且在数字签名和密钥的认证管理机制上有巧妙的设计,因此 PGP 成为几乎最流行的公钥加

密软件包，PGP 提供 5 种功能：鉴别、保密性、压缩、E-Mail 兼容性和分段功能，如表 7-7 所示。

表 7-7 PGP 的安全功能

功　　能	使用的算法	说　　明
鉴别	RSA 或 DSS、MD5 或 SHA	用 MD5 或 SHA 对消息散列并用发送者的私钥加密消息摘要
保密性	IDEA、CAST、3DES、Diffie-hellman 或 RSA	发送者产生一次性会话密钥，用会话密钥以 IDEA、CAST 或 3DES 加密消息，并用接收者的公钥以 Diffie-hellman 或 RSA 加密会话密钥
压缩	ZIP	使用 ZIP 压缩消息，以便于存储和运输
E-Mail 兼容性	Radix64 交换	对 E-Mail 应用提供透明性，将加密消息用 Radix64 变换成 ASCII 字符串
分段功能		为适应最大消息长度限制，PGP 实行分段并重组

1）鉴别

鉴别即使用数字签名，所使用的协议如下。

（1）发送者编制消息 M。

（2）用 SHA 或 MD5 产生一个 128 位的散列值 H。

（3）用发送者的 RSA 或 DSS 私钥对 H 签名。

（4）将 M||H 经 Z 压缩变换后发送。

（5）接收者将接收的数据进行逆变换，并用发送者公钥解密出 H。

（6）对 M 计算散列值，与 H 进行比较以验证签名。

2）保密性

采用 128 位密钥的 IDEA 算法（可用 CAST-128 或 3DES），64 位 CFB 模式，初始向量为全零。会话密钥一次性使用，所使用协议如下。

（1）发送者产生消息 M 和 128 位会话密钥。

（2）用会话密钥，使用 IDEA、CAST-128 或 3DES 对经 Z 压缩后的 M 加密。

（3）用接收者的公钥，使用 RSA 或 Diffie-Hellman 解密得到加密该会话密钥。

（4）接收者用会话密钥，使用 IDEA、CAST-128 或 3DES 解密并解压缩得到 M。

PGP 可以同时提供保密性和鉴别。它采用先签名后加密的方法，其优点在于存储消息明文的签名较为方便，第三方公证时，无须知道通信双方所使用的会话密钥。

3）压缩

压缩可以节省通信时间和存储空间，而且在加密前压缩，可以增强加密效果。PGP 中采用 PKZIP 算法。

4）E-Mail 兼容性

PGP 在保密性或鉴别功能下，输出的结果都是加密数据，即输出中的部分或全部为8 位串。许多 E-Mail 系统只允许使用 ASCII 文本。为此 PGP 采用 Radix64 变换，将 8 位串变为可打印的 ASCII 字符串。

5）分段

E-Mail 对消息长度都有限制，例如不超过 50KB。当消息大于此值时，PGP 将对其自动分段。分段在所有处理之后进行，故会话密钥和签名只在第一段开始部分出现。在接收时 PGP 将各段自动重组成原来的消息。

3. PEM

PEM(Privacy Enhanced Mail)是为 E-Mail 应用提供一个有关安全的 Internet 标准建议草案，一般不与 Internet 标准 SMTP(Simple Mail Transfer Protocol)结合使用。PEM 可广泛用于电子邮递，包括 X. 400。PEM 意图使密钥管理方法有广泛的适用性，允许用对称或公开密码体制实现。但实用以来，多采用公开密码体制。

PEM 由下述 4 个 RFC 文件规定，并于 1993 年发布了最后文本。

(1) RFC1421，Internet 中的 PEM：第 I 部分，消息加密和认证方法。

(2) RFC1422，Internet 中的 PEM：第 Ⅱ 部分，基于证书的密钥管理。

(3) RFC1423，Internet 中的 PEM：第 Ⅲ 部分，算法、模型和识别符。

(4) RFC1424，Internet 中的 PEM：第 Ⅳ 部分，密钥证实和有关服务。

这些 RFC 文件由属于 IETF 的 PEM 工作组负责，而后者又属于 IAB(Internet Architecture Board)。自 1985 年开始工作，由 IAB 的 Privacy and Security Research Group 负责起草工作。

PEM 的安全功能具有机密性、数据源认证、消息完整性和不可抵赖性。PEM 不支持一些与安全有关的服务，如访问控制、业务流量保密、路由控制、有关多个用户使用同一计算机的安全问题、消息回执和对回执的不可抵赖、与所查消息自动关联、消息副本检测、防止重放或其他面向数据流的服务。

1）密码算法

PEM 中的密码算法如表 7-8 所示。

表 7-8　PEM 中的密码算法

功　能	使用的算法	说　明
消息加密	DES-CBC	采用一次性会话密钥，会话密钥按 RSA 体制用接收者公钥加密，和消息一起送出
鉴别和签名	RSA 及 MD2 或 MD5	用 MD2 或 MD5 进行散列，用发送者密钥按 RSA 加密，和消息一起送出
鉴别(单钥)	DES-ECB 或 DES-EDE	用 MD2 或 MD5 进行散列，用 DES-ECB 及 MD2，MD5 或 DES-EDS(3DES)加密，和消息一起送出
单钥密钥管理	DES-ECB 或 DES-EDE	会话密钥以 DES-ECB 或 DES-EDE(3DES)加密，和消息一起送出
双钥密钥管理	RSA，MD2	建立公钥证书，用 MD2 对其散列。以收信人公钥按 RSA 对会话密钥加密，并于消息一起送出
E-Mail 兼容性	Radix64 变换	为对 E-Mail 应用提供透明性，已加密消息可用 Radix64 变换为 ASCII 字符串

PEM 提供了应用不同密码算法的格式，具有灵活性。和 MD2 与 MD5 一样，散列值均为 128 位。DES-EDE 是 ANSIX9. 17 建议的 3DES 应用模式(加密、解密、加密)，密钥为

56 * 2位。

2) PEM 中的密钥

表 7-9 中的 MIC 为消息完整性码(Message Integrity Code),IK(Inter Change Key)为收发共享密钥或公钥体制的公开私有密钥对,DEK(Data Encryption key)为一次性会话密钥。

表 7-9 PEM PEM 中的密钥用途

	对称密钥管理	公开密钥管理
用于加密的数据加密密钥(DEK)	消息文本、签署的 MIC 表示	消息文本
用于加密的交换密钥(IK)	DEK	DEK、MIC
发布人用于加密的单钥	公钥证书、散列值	发布人用于加密的单钥

3) PEM 消息发送和接收过程

消息发送处理分 4 步,如图 7-1 所示。

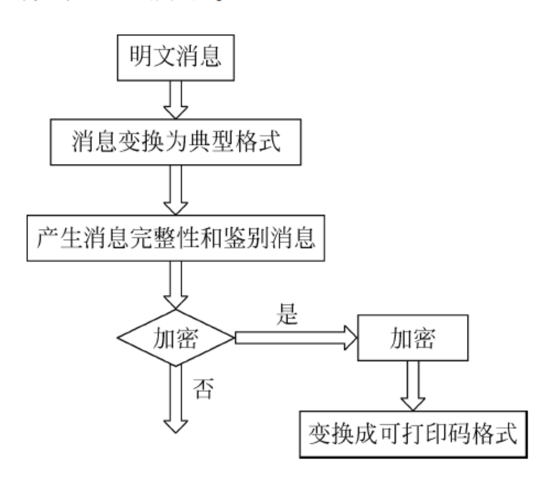


图 7-1 消息发送处理

(1) 将消息交换成典型格式,以适应兼容性和完整性要求。

(2) 产生消息完整性和鉴别消息。

(3) 对消息加密(可选)。

(4) 将其变换成可打印码格式(可选)。

PEM 的典型格式(canonical form)由消息头字段指明,称其为内容域字段(content-domain field),目前采用 SMTP 的 RFC 822 中规定的格式。

(1) 消息可由 7 位 ASCII 码中的任何字符组成,所有输入字符均被变换为 ASCII 码,每个 7 位码被安排在 8 位的后 7 位,最左位置为“0”。

(2) ASCII 的<CR><LF>序列用于限定行的终点。

(3) 报文每行最长含<CR><LF>在内,为 1000 个字符。大于此值的行将用<CR><LF>隔开。

PEM 的完整性和鉴别,即对典型格式用整个消息计算其 MIC,此计算可用对称或公开密码体制实现。

56＊2位。

2）PEM 中的密钥

表 7-9 中的 MIC 为消息完整性码(Message Integrity Code)，IK(Inter Change Key)为收发共享密钥或公钥体制的公开私有密钥对，DEK(Data Encryption key)为一次性会话密钥。

表 7-9 PEM PEM 中的密钥用途

	对称密钥管理	公开密钥管理
用于加密的数据加密密钥(DEK)	消息文本、签署的 MIC 表示	消息文本
用于加密的交换密钥(IK)	DEK	DEK、MIC
发布人用于加密的单钥	公钥证书、散列值	发布人用于加密的单钥

3）PEM 消息发送和接收过程

消息发送处理分 4 步，如图 7-1 所示。

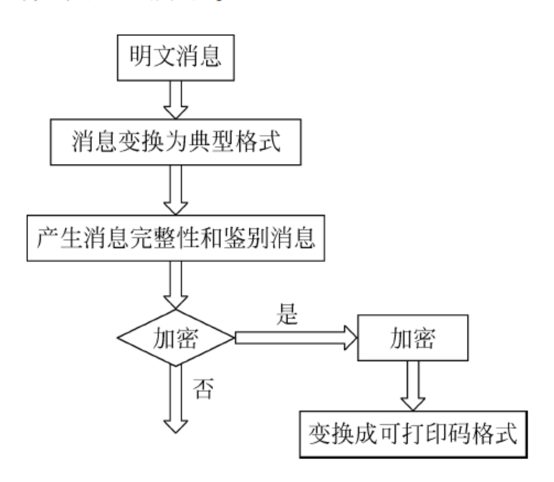


图 7-1 消息发送处理

(1) 将消息交换成典型格式，以适应兼容性和完整性要求。

(2) 产生消息完整性和鉴别消息。

(3) 对消息加密(可选)。

(4) 将其变换成可打印码格式(可选)。

PEM 的典型格式(canonical form)由消息头字段指明，称其为内容域字段(content-domain field)，目前采用 SMTP 的 RFC 822 中规定的格式。

(1) 消息可由 7 位 ASCII 码中的任何字符组成，所有输入字符均被变换为 ASCII 码，每个 7 位码被安排在 8 位的后 7 位，最左位置为“0”。

(2) ASCII 的< CR >< LF >序列用于限定行的终点。

(3) 报文每行最长含< CR >< LF >在内，为 1000 个字符。大于此值的行将用< CR >< LF >隔开。

PEM 的完整性和鉴别，即对典型格式用整个消息计算其 MIC，此计算可用对称或公开密码体制实现。

第 8 章　信息安全事件应急处理与灾难恢复

本章学习目标：

- 了解信息安全事件的基本概念。
- 了解信息安全事件应急处理与灾难恢复的过程。

8.1　信息安全事件

8.1.1　信息安全事件的定义

计算机系统常常会受到影响，从数据文件损坏到病毒，再到自然灾害，或者因自然灾害导致的停电，还有一些由恶意的技术活动（如创建病毒或系统黑客）导致的破坏事件。

计算机安全事件可能由计算机病毒、其他恶意代码、内部或外部的系统入侵者导致。它可以特指那些在没有技术专家响应时会造成严重损害的事件。计算机安全事件这种定义的不确定性太强，在不同的机构或计算环境中所表示的可能会有所不同。

2007 年 6 月 14 日《信息安全技术信息安全事件分类分级指南（GB/Z 20986—2007）》（以下简称《安全事件分类分级指南》）正式发布。《安全事件分类分级指南》为重要信息系统和基础信息网络的运营和使用单位以及信息安全主管部门处理信息安全事件提供了“事前准备、事中应对、事后处理”的基础指南，促进了各单位信息安全事件信息的交流和共享，提高了信息安全事件通报和应急响应的自动化程度和效率。在《安全事件分类分级指南》中分别对信息系统（information system）以及信息安全事件（information security incident）的概念进行了定义。

信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

信息安全事件是由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。信息安全事件的防范和处置是国家信息安全保障体系中的重要环节，也是重要的工作内容。

8.1.2　信息安全事件的分类

信息安全事件的分级和分类是快速有效处理信息安全事件的基础，是信息安全事件应急响应的基础。一般而言，信息安全事件可以是故意、过失或非人为原因引起的。

在《安全事件分类分级指南》中综合考虑信息安全事件的起因、表现、结果等，对信息安全事件进行了分类，将信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件共 7 个，每个基本分类分别包括若干个子类。表 8-1 是信息安全事件基本分类的一个汇总表。

表 8-1　信息安全事件分类汇总表

信息安全事件基本分类	相关子类
有害程序事件 (malware incidents)	计算机病毒事件(computer virus incidents)
	蠕虫事件(worms incidents)
	特洛伊木马事件(trojan horses incidents)
	僵尸网络事件(botnets incidents)
	混合攻击程序事件(blended attacks incidents)
	网页内嵌恶意代码事件(web browser plug-Ins incidents)
	其他有害程序事件(other malware incidents)
网络攻击事件 (network attacks incidents)	拒绝服务攻击事件(denial of service attacks incidents)
	后门攻击事件(backdoor attacks incidents)
	漏洞攻击事件(vulnerability attacks incidents)
	网络扫描窃听事件(network scan & eavesdropping incidents)
	网络钓鱼事件(phishing incidents)
	干扰事件(interference incidents)
	其他网络攻击事件(other network attacks incidents)
信息破坏事件 (information destroy incidents)	信息篡改事件(information alteration incidents)
	信息假冒事件(information masquerading incidents)
	信息泄露事件(information leakage incidents)
	信息窃取事件(information interception incidents)
	信息丢失事件(information loss incidents)
	其他信息破坏事件(other Information destroy incidents)
信息内容安全事件 (information content security incidents)	违反宪法和法律、行政法规的信息安全事件
	针对社会事项进行讨论、评论,形成网上敏感的舆论热点,出现一定规模炒作的信息安全事件
	组织串连、煽动集会游行的信息安全事件
	其他信息内容安全事件
设备设施故障 (facilities faults)	软硬件自身故障(software and hardware faults)
	外围保障设施故障(periphery safeguarding facilities faults)
	人为破坏事故(man-made destroy accidents)
	其他设备设施故障(other facilities faults)
灾害性事件 (disaster incidents)	包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件
其他信息安全事件 (other incidents)	不能归为以上 6 个基本分类的信息安全事件

本书下面将分别对有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障这 5 类信息安全事件做详细介绍。

1. 有害程序事件

有害程序事件是指蓄意制造、传播有害程序,或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序,有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性,或影响信息系统的正常运行。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌

恶意代码事件和其他有害程序事件7个子类,各子类事件的情况分别如下所述。

(1) 计算机病毒事件是指蓄意制造、传播计算机病毒,或是因受到计算机病毒影响而导致的信息安全事件。计算机病毒是指编制或者在计算机程序中插入的一组计算机指令或者程序代码,它可以破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制。

(2) 蠕虫事件是指蓄意制造、传播蠕虫,或是因受到蠕虫影响而导致的信息安全事件。蠕虫是指除计算机病毒以外,利用信息系统缺陷,通过网络自动复制并传播的有害程序。

(3) 特洛伊木马事件是指蓄意制造、传播特洛伊木马程序,或是因受到特洛伊木马程序影响而导致的信息安全事件。特洛伊木马程序是指伪装在信息系统中的一种有害程序,具有控制该信息系统或进行信息窃取等对该信息系统有害的功能。

(4) 僵尸网络事件是指利用僵尸工具软件,形成僵尸网络而导致的信息安全事件。僵尸网络是指网络上受到黑客集中控制的一群计算机,它可以被用于伺机发起网络攻击,进行信息窃取或传播木马、蠕虫等其他有害程序。

(5) 混合攻击程序事件是指蓄意制造、传播混合攻击程序,或是因受到混合攻击程序影响而导致的信息安全事件。混合攻击程序是指利用多种方法传播和感染其他系统的有害程序,可能兼有计算机病毒、蠕虫、木马或僵尸网络等多种特征。混合攻击程序事件也可以是一系列有害程序综合作用的结果,例如一个计算机病毒或蠕虫在侵入系统后安装木马程序等。

(6) 网页内嵌恶意代码事件是指蓄意制造、传播网页内嵌恶意代码,或是因受到网页内嵌恶意代码影响而导致的信息安全事件。网页内嵌恶意代码是指内嵌在网页中,未经允许由浏览器执行,影响信息系统正常运行的有害程序。

(7) 其他有害程序事件是指不能包含在以上6个子类之中的有害程序事件。

【有害程序事件举例】

2016年4月,CNCERT监测发现,一个名为Ramnit的网页恶意代码被挂载在境内近600个党政机关、企事业单位网站上,一旦用户访问网站就有可能受到挂马攻击,对访问网站用户的PC主机构成安全威胁。Ramnit恶意代码是一个典型的VBScript蠕虫病毒,可通过网页挂马的方式进行传播,当用户浏览含有Ramnit恶意代码的HTML页面时,单击加载ActiveX控件,用户主机就很有可能受到恶意代码的感染。

Ramnit主要是在用户的TEMP文件夹中植入一个名为svchost.exe的二进制文件并执行关联的ActiveX控件,受感染的用户主机会试图连接到与Ramnit相关的一个木马控制服务器——http://fget-career.com。根据CNCERT监测情况分析,Chrome和Firefox浏览器用户不会受到恶意代码的影响,较高版本的IE浏览器也会对此类ActiveX控件进行告警提示而不是自动执行。所以,受影响的主要是较低版本的IE浏览器。建议IE浏览器用户在访问互联网时做好IE安全设置(建议设置为中、高安全级别),禁止执行不明来源的ActiveX控件。

该事件也提醒用户IE浏览器需要进行安全设置(可设置为中、高安全级别),对于是否执行来源不明的ActiveX控件,将由用户自己做出选择,或者可以禁止执行来源不明的ActiveX控件;尽量避免使用老版本的IE浏览器;当然经常杀毒、清理计算机中的垃圾也是必要的。企业需要注意升级单位网站,及时提升服务器性能、强化服务器;需要定期进行

网站安全检查，通过渗透等办法排查潜在问题，防患于未然。

2. 网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。

网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件 7 个子类，各子类事件的情况分别如下所述。

(1) 拒绝服务攻击事件是指利用信息系统缺陷或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的的信息安全事件。

(2) 后门攻击事件是指利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施的攻击的信息安全事件。

(3) 漏洞攻击事件是指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件。

(4) 网络扫描窃听事件是指利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征而导致的信息安全事件。

(5) 网络钓鱼事件是指利用欺骗性的计算机网络技术，使用户泄露重要信息而导致的信息安全事件。例如，利用欺骗性电子邮件获取用户银行账号、密码等。

(6) 干扰事件是指通过技术手段对网络进行干扰，或对广播电视有线、无线传输网络进行插播，对卫星广播电视信号非法攻击等导致的信息安全事件。

(7) 其他网络攻击事件是指不能被包含在以上 6 个子类之中的网络攻击事件。

【网络攻击事件举例】

2016 年 3 月，全球有 2/3 的网站服务器使用的开源的加密工具 OpenSSL 爆出新的安全漏洞——水牢漏洞，这一漏洞允许黑客攻击网站，并读取密码、信用卡账号、商业机密和金融数据等加密信息，对全球网站产生巨大的安全考验。我国有十万余家网站受到影响。

这次事件之所以被如此高度关注，除了影响范围很大外，也是因为 OpenSSL 这一互联网基础组件目前已经成为众矢之的。从 2014 年的心脏滴血漏洞开始，OpenSSL 不断被爆出大范围漏洞，虽然这次漏洞的利用难度很大，许多软件早已通过禁用 SSLv2 规避了这个漏洞，但有关开源软件的安全话题被再次广泛讨论。一方面因为其开源性，黑客更容易通过对源代码的研究来发现漏洞；另一方面，大多数开源软件因为没有商业公司支撑，出现漏洞，用户无法在第一时间被告知，给漏洞的修补带来了极大的困难。

这次事件也提醒作为用户，定期扫描、及时升级软件到最新版本、仔细核查软件配置、关闭不安全选项、关注安全公司的威胁情况播报，是避免此类漏洞殃及自身的有效手段。

3. 信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄露、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息

泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件6个子类,各子类事件的情况分别如下。

(1) 信息篡改事件是指未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件,例如网页篡改等导致的信息安全事件。

(2) 信息假冒事件是指通过假冒他人信息系统收发信息而导致的信息安全事件,例如网页假冒等导致的信息安全事件。

(3) 信息泄露事件是指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件。

(4) 信息窃取事件是指未经授权用户利用可能的技术手段恶意主动获取信息系统中信息而导致的信息安全事件。

(5) 信息丢失事件是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件。

(6) 其他信息破坏事件是指不能被包含在以上5个子类之中的信息破坏事件。

【信息破坏事件举例】

2016年2月1日,浙江警方通报了半年以来整治网络违法犯罪行为的15起典型案例,其中,嘉兴平湖警方破获的一起网络黑客案件中,犯罪团伙利用互联网上非法传播的非淘宝用户账号和密码对淘宝账号进行“撞库”匹配,用于抢单等黑客行为,涉案金额高达200余万元。此次事件并非是淘宝被攻击导致的账号泄露。通过案件调查发现,是该团伙于2015年10月14日至16日通过租用阿里云服务器进行“撞库”,犯罪团伙利用手中已有的非淘宝账号对淘宝网进行了9900多万次比对,匹配后发现有2059万账号真实存在,占比竟然高达20.8%。2059万个账号中,黑客比对后曾尝试利用其他平台进行登录(俗称“撞库”),绝大多数登录行为遭到淘宝网的拦截因而未遂,但是大部分账号还是被不法分子用于抢单等恶意行为。

“撞库”是互联网较常见的黑客行为,以大量的用户数据为基础,利用用户相同的注册习惯(相同的用户名和密码),尝试登录其他的网站。被撞库网站和用户都是黑客行为的受害者,用户在A网站被盗的账户和密码被用来登录B网站,因为很多用户在不同网站使用的是相同的账号和密码,因此可以获取用户在B网站的用户账号和密码,从而达到目的。因此一旦某个网站的用户数据库泄露,将导致该用户在多个网站的资产受损。

事件提醒

企业需要有完备的防范措施,对于被撞库的账号用户,需要第一时间进行安全提示和密码修改提醒,并采取临时保护措施,直至用户完成密码修改;寻求更加主动有效的防护技术,化被动防御为主动防御。

用户需要注意,不要在多个网站使用同一套账号和密码,若使用同一套账号和密码,则相当于给不法分子配了一把“万能钥匙”,应尽量做到在每一个网站有独立的用户名与密码,并定期更新;计算机中一定要安装安全软件,这样能够一定限度降低用户被攻击的风险,保证用户信息的安全。应使用正版软件,使用“盗版”软件、“破解”软件计算机中可能会被植入各类木马病毒文件,极易泄露个人隐私;遇事要冷静,先确认事情的真伪,遇到不明支付短

信等情况不要慌张，发现资金异常应立即联系银行或选择报案，以防止造成财产损失。

4. 信息内容安全事件

信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件。信息内容安全事件包括以下 4 个子类，各子类事件的情况分别如下所述。

(1) 违反宪法和法律、行政法规的信息安全事件。

(2) 针对社会事项进行讨论、评论，形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件。

(3) 组织串连、煽动集会游行的信息安全事件。

(4) 其他信息内容安全事件。

【信息内容安全事件举例】

2015 年 4 月 28 日的山东非法疫苗案经澎湃新闻刊发后，引发持续关注。据报道，该案疫苗未经严格冷链存储运输，便销往 24 个省市，案值 5.7 亿元。报道刊发后，该消息迅速弥漫全网，连续多日占据热门排名。该事件的网上舆情呈现出又高又热的紧张态势，可能存在以下原因：一是疫苗直接牵涉孩子，容易持续刺激年轻父母而造成强烈的恐慌心理；二是受专业知识、医疗背景等客观条件限制，很容易将冷藏的失效疫苗视同有毒疫苗，不断触及人们的情感痛点；三是段子手、公关公司、营销号趁机"碰瓷"热点，借势营销；四是受现实多重因素影响，舆论中关于监管部门与违法企业间的责任界限较为模糊，提供讨论、猜忌空间。

5. 设备设施故障事件

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为地使用非技术手段有意或无意地造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障 4 个子类，各子类事件的情况分别如下。

(1) 软硬件自身故障是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件。

(2) 外围保障设施故障是指由于保障信息系统正常运行所必需的外部设施出现故障而导致的信息安全事件，例如电力故障、外围网络故障等导致的信息安全事件。

(3) 人为破坏事故是指人为蓄意地对保障信息系统正常运行的硬件、软件等实施窃取、破坏造成的信息安全事件；或由于人为地遗失、误操作以及其他无意行为造成信息系统硬件、软件等遭到破坏，影响信息系统正常运行的信息安全事件。

(4) 其他设备设施故障是指不能被包含在以上 3 个子类之中的设备设施故障而导致的信息安全事件。

【设备设施故障事件举例】

2015 年 12 月 23 日，乌克兰伊万诺-弗兰科夫斯克地区(人口 140 万)大约一半的家庭断电数小时。据乌克兰新闻通讯社报道，这次大规模停电事件，是由于黑客在乌克兰国家电网

中植入了恶意软件,从而导致发电站意外关闭。这是首次由黑客攻击行为导致的大规模停电事件,引起了公众的极大恐慌。黑客使用的高破坏性的恶意软件,攻击并感染了乌克兰至少三个地区电力部门的基础设施,导致发电设备产生故障。

ESET公司的研究人员已经证实,乌克兰电力部门的计算机中被植入了BlackEnergy恶意软件,该软件最初于2007年被发现,并通过不断更新,添加了许多新功能,其中包括使被感染的计算机无法重启的功能。最近,ESET公司发现,BlackEnergy恶意软件再次更新,并增加了被称为KillDisk的组件,它能够破坏计算机硬盘驱动器的关键部分,因此可以用于实施针对新闻媒体企业及电力行业的攻击。

8.1.3 信息安全事件分级

1. 信息安全事件分级要素

对信息安全事件的分级主要考虑3个要素:信息系统的重要程度、系统损失和社会影响。各要素的程度衡量导图如图8-1所示。

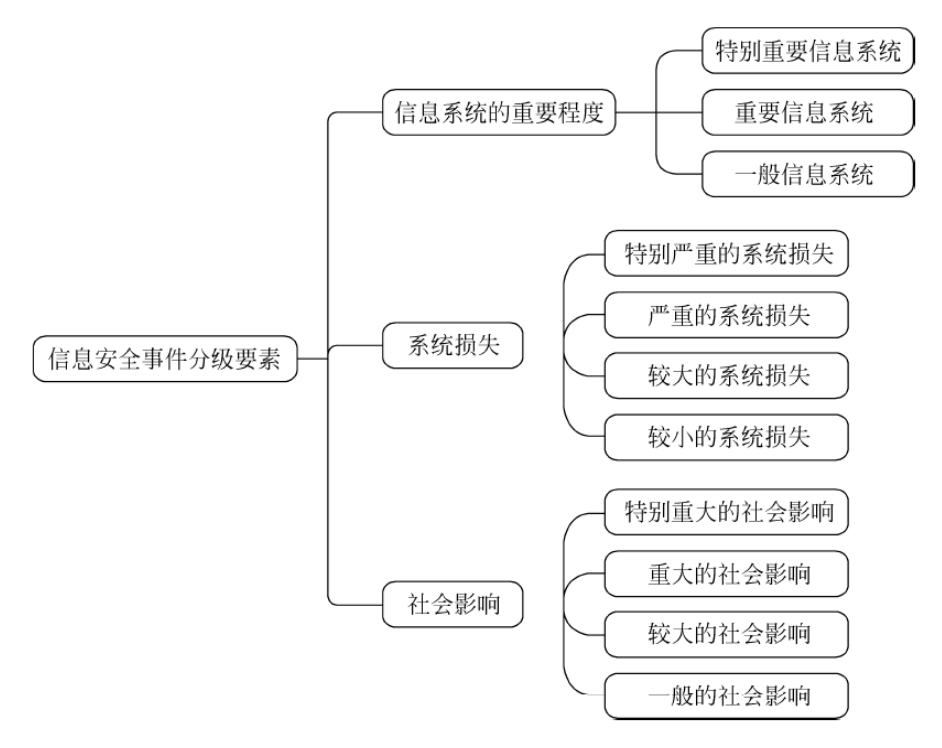


图8-1 信息安全分级要素导图

1)信息系统的重要程度

信息系统的重要程度主要考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性以及业务对信息系统的依赖程度,划分为特别重要信息系统、重要信息系统和一般信息系统。

2)系统损失

系统损失是指由于信息安全事件对信息系统的软硬件、功能及数据的破坏,导致系统业务中断,从而给事发组织所造成的损失,其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价,划分为特别严重的系统损失、严重的系统损失、较大的系统损失

和较小的系统损失，这里对各损失程度做一个说明。

(1) 特别严重的系统损失。造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的。

(2) 严重的系统损失。造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的。

(3) 较大的系统损失。造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的。

(4) 较小的系统损失。造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

3) 社会影响

社会影响是指信息安全事件对社会所造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响，划分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响，这里对各种影响说明如下。

(1) 特别重大的社会影响。波及一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。

(2) 重大的社会影响。波及一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益。

(3) 较大的社会影响。波及一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。

(4) 一般的社会影响。波及一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

2. 信息安全事件的级别划分

根据信息安全事件的分级要素所达到的情况和描述，将信息安全事件划分为 4 个级别：特别重大事件、重大事件、较大事件和一般事件。表 8-2 是信息安全事件 4 个级别情况的描述汇总。

表 8-2　信息安全事件分级一览表

信息安全事件等级	描　　述	分级要素情况
特别重大事件（Ⅰ级）	能够导致特别严重影响或破坏的信息安全事件	会使特别重要信息系统遭受特别严重的系统损失
		产生特别重大的社会影响
重大事件（Ⅱ级）	能够导致严重影响或破坏的信息安全事件	会使特别重要信息系统遭受严重的系统损失
		会使重要信息系统遭受特别严重的系统损失
		产生重大的社会影响

续表

信息安全事件等级	描　　述	分级要素情况
较大事件（Ⅲ级）	能够导致较严重影响或破坏的信息安全事件	会使特别重要信息系统遭受较大的系统损失
		会使重要信息系统遭受严重的系统损失
		一般信息系统遭受特别严重的系统损失
		产生较大的社会影响
一般事件（Ⅳ级）	不满足以上条件的信息安全事件	会使特别重要信息系统遭受较小的系统损失
		会使重要信息系统遭受较大的系统损失
		一般信息系统遭受严重或严重以下级别的系统损失
		产生一般的社会影响

8.2　信息安全事件应急响应与处置过程

8.2.1　应急响应的概念

应急响应(emergency response 或 incident response)是指一个组织为了应对各种信息安全突发事件的发生所做的准备以及在事件发生后所采取的措施。应急响应旨在减少信息安全事件对组织和业务的影响,它体现了一个组织驾驭事件的能力。一个组织在威胁出现时能够迅速地对威胁做出反应,在发生信息安全事件时拥有一个行之有效的处置手段以响应事件,就有可能有效地减少和降低恢复系统的代价。

在现有的各种网络安全模型中,关于信息安全事件处理都被归结到应急响应这样一个重要的环节中。因为对事件的应急响应是整个安全防范体系中最后可以依赖的防护手段,所以要求应急响应的事件处理必须能够找到一种通用的策略,实现对当前发生的已知的攻击事件和将来可能发生的新的未知攻击事件的处理。

8.2.2　应急响应计划及流程

1. 应急响应计划的定义

应急响应计划(emergency response plan)是指组织为了应对突发或重大信息安全事件而编制的、对包括信息系统运行在内的业务运行进行维持或恢复的策略和规程。这里的事件包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等。

信息系统容易受到各种已知和未知的威胁而导致有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等信息安全事件的发生。虽然很多信息安全事件可以通过技术的、管理的、操作的方法予以消减,但目前没有任何一种信息安全策略或防护措施,能够对信息系统提供绝对的保护。即使采取了防护措施,仍可能存在残留的弱点,使得信息安全防护变得无效,从而导致业务中断、系统宕机、网络瘫痪等信息安全事件发生,并对组织和业务运行产生直接或间接的负面影响。因此,为了减小信息安全事件

对组织和业务的影响，应制订有效的信息安全应急响应计划。

2. 应急响应计划文档

应急响应计划文档应包含总则、角色及职责、预防和预警机制、应急响应流程、应急响应保障措施、附件 6 个基本要素。

1）总则

总则提供了重要的背景或相关信息，使应急响应计划更容易理解、实施和维护。通常这部分包括编制目的、编制依据、适用范围、工作原则等。

（1）编制目的。介绍制订信息安全应急响应计划的原因和目标。

（2）编制依据。说明编制信息安全应急响应计划的依据。

（3）适用范围。说明计划的作用范围，解决哪些问题，不解决那些问题。

（4）工作原则。确定应急响应计划组织和实施原则。

2）角色及职责

组织应结合本单位日常机构建立信息安全应急响应的工作机构，并明确其职责。应急响应的工作机构由管理、业务、技术和行政后勤等人员组成，一般来说，按角色可划分为 5 个功能小组：应急响应领导小组、应急响应技术保障小组、应急响应专家小组、应急响应实施小组和应急响应日常运行小组等。表 8-3 列出了各工作小组的工作职责。在实际中，可以不必专门成立对应的功能小组，组织可以根据自身情况由其具体的某个、某几个部门或部门中的某几个人担当其中的一个或几个角色。

表 8-3　应急响应工作小组的工作职责

功能小组	工作职责
应急响应领导小组	（1）对应急响应工作的承诺和支持，包括发布正式文件、提供必要资源（人、财、物）； （2）审核并批准应急响应策略； （3）审核并批准应急响应计划； （4）批准和监督应急响应计划的执行； （5）启动定期评审、修订应急响应计划； （6）负责组织的外部协作工作
应急响应技术保障小组	（1）制定信息安全事件技术应对表； （2）制定信息安全事件区域技术应对表； （3）制定具体角色和职责分工细则； （4）制定应急响应协同调度方案； （5）考察和管理相关技术基础
应急响应专家小组	（1）对重大信息安全事件进行评估，提出启动应急响应级别的建议； （2）研究分析信息安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议； （3）分析信息安全事件原因及造成的危害，为应急响应提供技术支持

续表

功能小组	工 作 职 责
应急响应实施小组	(1) 分析应急响应需求(如风险评估、业务影响分析等); (2) 确定应急响应策略和等级; (3) 实现应急响应策略; (4) 编制应急响应计划文档; (5) 实施应急响应计划; (6) 组织应急响应计划的测试、培训和演练; (7) 合理部署和使用应急响应资源; (8) 总结应急响应工作,提交应急响应总结报告; (9) 执行应急响应计划的评审、修订任务
应急响应日常运行小组	(1) 协助灾难恢复系统实施; (2) 备份中心日常管理; (3) 备份系统的运行和维护; (4) 应急监控系统的运作和维护; (5) 参与和协助应急响应计划的测试、培训和演练; (6) 维护和管理应急响应计划文档; (7) 信息安全事件发生时的损失控制和损害评估

组织可聘请具有相应资质的外部专家协助应急响应工作,也可委托具有相应资质的外部机构承担实施小组以及日常运行小组的部分或全部工作。在聘请外部专家协助应急响应工作或者委托外部机构承担部分或者全部应急响应工作时,需要和其签订相关协议(例如签订有关信息保密要求等)。

3) 预防和预警机制

组织应加强信息安全监测、分析和预警工作,建立信息安全事件报告和通报制度,发生信息安全事件的单位或者部门应当在信息安全事件发生后立即向应急响应日常运行小组报告,这是一种防御性的方法。在可行和比较划算的情况下,防御性方法要比信息安全事件发生后进行应急响应更好。有很多防御性控制措施可供选择,它依赖于信息系统的类型和配置。

预防和预警机制应被记录在应急响应计划中,应对系统相关的人员进行培训,使他们明确如何以及何时使用预防和预警机制。预防和预警机制应得到维护以处于良好状态,从而确保其在信息安全事件中的有效性。积极推行信息安全等级保护制度,基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复(灾难恢复的内容将在 8.3 节做详细介绍)。

4) 应急响应流程

应急响应流程规定了信息安全事件发生后应采取的工作流程和相应条款,目的是保证应急响应能够有组织地执行,从而最大限度地保证应急响应的有效性,具体内容在 8.2.3 节做详细介绍。

5) 应急响应保障措施

应急响应保障措施是信息安全应急响应计划的重要组成部分,是保证信息安全事件发生后能够快速有效地实施应急响应计划的关键要素。一般情况下,人力保障、物质保障和技

术保障这三个方面是必要的，组织也可以根据自己的性质和需求考虑调整增加其他方面的保障措施来保证应急响应计划的制订符合组织的实际情况。

6）附件

应急响应计划的附件提供了计划主体不包含的关键细节。常见的应急响应计划附件包括：具体的组织体系结构和人员职责；应急响应计划各小组成员的联络信息；供应商联络信息，包括离站存储和备用站点的外部联系点（POC）；系统恢复或处理的标准操作规程和检查列表；支持系统运行所需的硬件、软件、固件和其他资源的设备与系统需求清单，清单中的每个条目应包含型号或版本号、规定说明和数全等详细内容；供应商服务水平协议（SLA）、与其他机构的互惠协议和其他关键记录；备用站点的描述和说明；在计划制订前进行的 BIA，包含关于系统各部分的相互关系、风险、优先级别等；应急响应计划文档的保存和分发方法。

3. 应急响应计划的制订

信息安全应急响应计划的制订一般包含应急响应计划的编制准备，编制应急响应计划文档及应急响应计划的测试、培训、演练和维护 3 个阶段。

信息安全应急响应计划的制订也是一个周而复始、持续改进的过程，应急响应计划为信息安全事件发生后的应急响应提供了指导策略和规程，否则，应急响应将陷入混乱，而毫无章法的应急响应有可能造成比信息安全事件本身更大的损失。另外，应急响应可能发现事前应急响应计划的不足，从而吸取教训，进而进一步完善应急响应计划。所以，制订应急响应计划与应急响应是一个循环反复、相互补充和相互促进的过程。应急响应计划与应急响应的关系如图 8-2 所示。

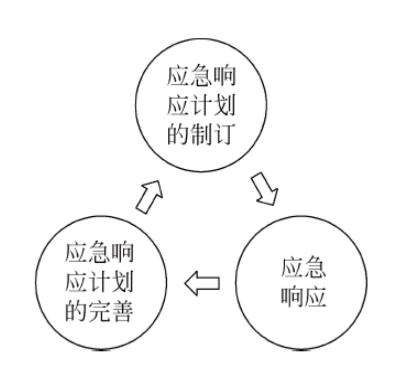


图 8-2　应急响应计划与应急响应的关系

8.2.3　信息安全应急响应流程

信息安全应急处理是指通过制订应急响应计划使得影响信息系统安全的安全事件能够得到及时响应，并在安全事件一旦发生后进行标示、记录、分类和处理，直到受影响的业务恢复正常运行的过程。

应急响应流程描述并规定了信息安全事件发生后应采取的工作流程和相应条款，目的是保证应急响应能够有组织地执行，从而最大限度地保证应急响应的有效性。信息安全事件应急响应流程中包含信息安全事件通报、信息安全事件评估、应急启动、应急处理和后期处理，如图 8-3 所示。

1. 信息安全事件的通报

1）信息通报。

（1）组织内信息通报。在信息安全事件发生后，应通知应急响应日常运行小组使其能够确定事态的严重程度和下一步将要采取的行动。在损害评估完成后，应通知应急响应领导小组。通知策略应定义信息安全事件发生后人员无法联络时的规程。

（2）组织外信息通报。信息安全事件发生后，应将相关信息及时通报给受到负面影响

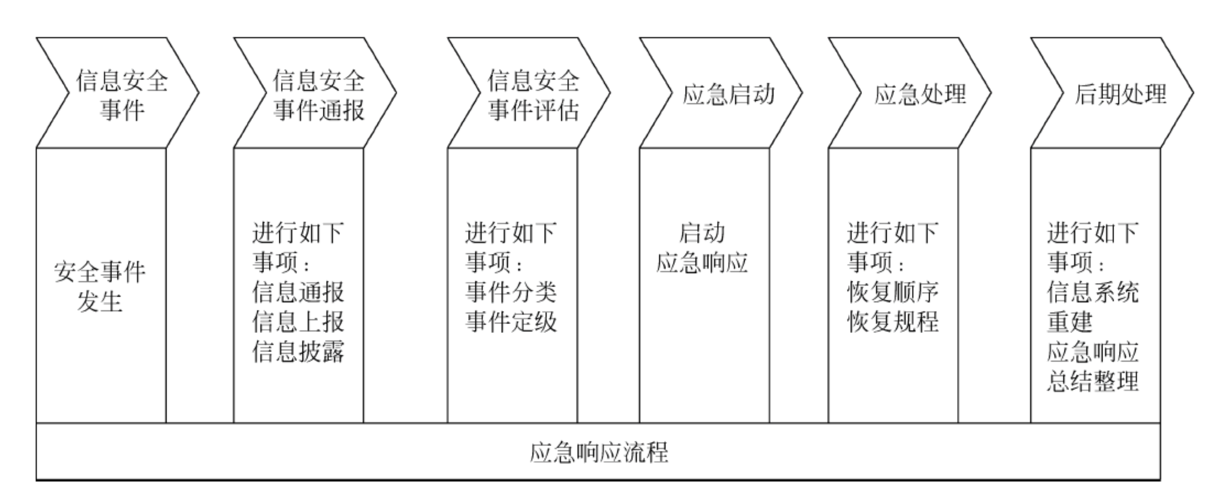


图 8-3 信息安全事件应急响应流程

的外部机构、互联的单位系统以及重要客户，同时根据应急响应的需要，应将相关信息准确通报给相关设备及服务提供商、电信、电力等外部组织，以获得适当的应急响应支持。对外信息通报应符合组织的对外信息发布策略。

2）信息上报

信息安全事件发生后，应按照相关规定和要求，及时将情况上报相关单位或者部门。

3）信息披露

信息安全事件发生后，根据信息安全事件的严重程度，组织应指定特定的小组及时向新闻媒体发布相关信息，指定的小组应严格按照组织相关规定和要求对外发布信息，同时组织内其他部门或者个人不得随意接受新闻媒体采访和对外发表自己的看法。

2. 信息安全事件评估

信息安全事件发生后，应急响应日常运行小组需要对信息安全事件进行评估，确定信息安全事件的类别与级别。这个阶段要进行事件的分类和分级，关于信息安全事件的分类与分级在 8.1.2 节和 8.1.3 节已经进行了详细介绍。

3. 应急启动

应急启动具体操作应遵循下面的规则。

(1) 启动原则。快速、有序。

(2) 启动依据。

一般而言，对于导致业务中断、系统宕机、网络瘫痪等突发或重大信息安全事件应立即启动应急。但由于组织规模、构成、性质等的不同，不同组织对突发或重大信息安全事件的定义会有差异，因此，各组织的应急启动条件也会不同。

一般可以考虑人员安全和(或)设施损失的程度；系统损失的程度(如物理的、运作的或成本的)；系统对于组织使命的影响程度(如保护资产的关键基础设施)；预期的中断持续时间等。只有当损害评估的结果显示一个或多个系统启动条件被满足时，应急响应计划才应被启动。

(3) 启动方法。

由应急响应领导小组发布应急响应启动令。应急响应启动后应急响应领导小组要对人

力、财力、物力到位情况实施检查与督察，并记录实际发生情况。

4. 应急处理

启动应急响应计划后应立即采取相关措施抑制信息安全事件影响，避免造成更大损失。在确定有效控制了信息安全事件影响后开始恢复操作，恢复阶段的行动集中于建立临时业务处理能力、修复原系统损害、在原系统或新设施中恢复运行业务能力等应急措施。要遵循一定的恢复顺序和恢复规程。

1）恢复顺序

当恢复复杂系统时，恢复进程应反映出业务影响分析中确定的系统优先顺序。恢复的顺序应反映出系统允许的中断时间，以避免对相关系统及业务的重大影响。

2）恢复规程

为了进行恢复操作，应急响应计划应提供恢复业务能力的详细规程。规程应被设定给适当的恢复小组并且通常涉及以下行动。

(1) 获得访问受损设施和(或)地理区域的授权。

(2) 通知相关系统的内部和外部业务伙伴。

(3) 获得所需的办公用品和工作空间。

(4) 获得安装所需的硬件部件。

(5) 获得装载备份介质。

(6) 恢复关键操作系统和应用软件。

(7) 恢复系统数据。

(8) 成功运行备用设备。

5. 后期处理

1）信息系统重建

在应急工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常的工作。通过统计各种数据，查明原因，对信息安全事件造成的损失和影响以及恢复重建能力进行分析评估，认真制订恢复重建计划，迅速组织实施信息系统重建。

2）应急响应总结整理

应急响应总结是应急处理之后应进行的工作，具体包括以下工作。

(1) 分析和总结事件发生原因。

(2) 分析和总结事件现象。

(3) 评估系统的损害程度。

(4) 评估事件导致的损失。

(5) 分析和总结应急处理记录。

(6) 评审应急响应措施的效果和效率，并提出改进建议。

(7) 评审应急响应计划的效果和效率，并提出改进建议。

8.2.4　信息安全事件应急处理方法

随着互联网业务的快速发展，每年都有新的服务系统的安全漏洞被黑客发掘出来实施网络攻击。从根本上讲，在互联网的现实环境中是不存在绝对安全的系统的，任何一个系统

总是存在被攻陷的可能性。事实上很多时候恰恰是在系统被攻陷后,人们才得以发现系统中存在的薄弱环节,进而把系统的安全防护提高到一个更高的水平。因此,如何处理安全事件是安全防范过程中一个不可回避的重要问题。

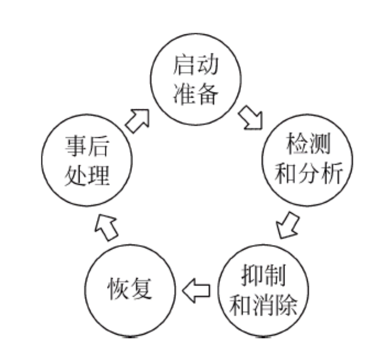


图 8-4 信息安全事件应急处理关键阶段

信息安全事件应急处理是指通过制订应急计划,使得影响信息系统安全的安全事件能够得到及时响应,并在安全事件一旦发生后进行标示、记录、分类和处理,直到受影响的业务恢复正常运行的过程。信息安全事件应急处理中有 5 个关键阶段,如图 8-4 所示

1. 启动准备阶段

该阶段的目标是对信息安全事件做出初步的动作和响应,根据获得的初步材料和分析结果,预估事件的范围和影响程度,制定进一步的响应策略,并且保留相关证据。该阶段有 4 个重要的控制点:应急响应需求界定;服务合同或协议签订;应急服务方案制订;人员和工具准备。

启动阶段包括建立和培训安全事件响应小组并获得必要的工具和资源。在准备工作中,组织也要以风险评估的结果为基础,通过选择和实施一套控制措施来限制安全事件的发生次数。但是即使在实施了安全控制措施后,残余风险依然不可避免,而且没有哪种控制措施是绝对安全的,所以对破坏网络安全的行为要进行检测,一旦安全事件发生要对组织发出报警。针对安全事件的严重程度,组织可以采取行动,通过对安全事件进行限制并最终从中恢复来减缓安全事件所造成的影响。在安全事件得到适当处理后,组织要提交一份报告,详细描述安全事件的起因、造成的损失以及以后对这类安全事件所应采取的防范措施和步骤。

2. 检测和分析阶段

该阶段的目标是对信息安全事件做出初步的动作和响应,根据获得的初步材料和分析结果,预估事件的范围和影响程度,制定进一步的响应策略,并且保留相关证据。该阶段有 3 个重要控制点:检测对象及范围确定;检测方案确定;检测实施。

1)检测对象及范围确定

信息安全事件的发生方式多种多样,所以想要制定一个具体的综合流程来处理每一件安全事件是不切实际的。信息安全事件响应过程中最困难的一步是准确检测并评估可能的安全事件,即确定一个安全事件是否会发生,如果发生,那么它属于什么类型、影响程度以及影响范围。

一般信息安全事件的发生都是有事件征兆的。事件征兆可以分为两类:前兆和迹象。前兆是指未来可能发生的安全事件的征兆,而迹象是指已经发生或正在发生的安全事件的征兆。前兆和迹象可以通过许多不同的来源来检测前兆和迹象,最常用的有计算机安全软件的告警、日志、公共渠道获取的信息。

2)检测方案确定

对安全事件进行分析和验证是很困难的。下面的一些建议将使安全事件的分析更简便有效:描述网络和系统的特征;了解正常行为;使用集中式日志并建立日志保存政策;开展安全事件关联分析;保证所有主机时钟同步;维护和使用信息知识库;利用因特网搜索引擎进行查找;使用数据包监听工具来获取更多信息;考虑数据简化;经验是不可代替的;

向其他人寻求帮助。

一旦安全事件响应小组怀疑正在发生或已经发生了安全事件，要立即记录有关该安全事件的全部事实。日志簿是一个简单有效的介质方法。把系统事件、电话交谈记录下来并观察其中变化，可以使问题处理更有效、更系统并且更少犯错误。从安全事件被发现到处理完毕过程中所采取的每一个步骤都应该加以记录，并注明时间。按照安全事件当前和潜在的技术影响与受影响资源的关键程度这两个因素来对安全事件的处理进行优先排序。

3）检测实施

当安全事件被分析完毕并优先排序之后，及时的报告和通知可以使相关人员发挥其作用，目前合作处理安全事件可能是最好的方法。

3. 抑制和消除阶段

抑制和消除阶段的目标是限制攻击的范围，抑制潜在的或进一步的攻击和破坏，在事件被抑制之后，通过对有关恶意代码或行为的分析结果找出导致安全事件发生的根源，并予以彻底消除。该阶段有 3 个重要控制点：抑制策略的选择；证据收集和处理；抑制消除实施。

1）抑制策略的选择

抑制策略一般随安全事件类型的不同而不同。例如，针对邮件病毒感染事件的限制策略和针对基于网络的分布式拒绝服务的限制策略就很不一样。抑制策略的选择可以根据资源的潜在破坏和丢失、证据的保存需求、服务的可用性（如网络连接、对外提供的服务）执行策略所需的资源和时间、策略的有效性（如部分限制了安全事件、完全限制了安全事件）、解决方案的持续时间（如紧急工作区需要在 4 小时内拆除、临时工作区需要在 2 周内拆除）等来确定。

2）证据收集和处理

从计算资源中收集证据有很大的困难。通常人们倾向于一旦怀疑发生了安全事件，就从相关系统中寻找证据。许多安全事件都会引发一系列的动态事件，初始系统快照对找出问题及其来源比这一阶段可以采取的大多数其他行动帮助更大。从证据的角度看，获得系统快照比事后让安全事件处理人员、系统管理员及其他人员在调查中漫不经心地提供机器状态要好得多。

3）抑制消除实施

识别攻击者过程中最常采取的方法有确认攻击者的 IP 地址、扫描攻击者的系统、使用网络搜索引擎查找攻击者、使用安全事件数据库、对攻击者可能的通信信道进行监视。

4. 恢复阶段

该阶段的目标是将信息安全事件所涉及的系统还原到正常状态。该阶段有 2 个重要控制点：恢复方法确定；恢复系统。

恢复工作通常会涉及以下活动：从备份上对系统进行恢复、从头重建系统、用干净的版本来替换被破坏的文件、安装补丁、更换口令并加强网络边界安全（如防火墙规则集、边界路由器的访问控制列表）。最好采用更高级别的系统日志或网络监视作为恢复过程的一部分。

在 8.3 节和 8.4 节将介绍信息系统灾难恢复的相关内容，这也是恢复阶段比较重要的环节和方法。

5. 事后处理

该阶段的目标是回顾信息安全事件处理的全过程，整理与事件相关的各种信息，并尽可能地把所有情况记录到文档中。该阶段有 2 个重要控制点：总结；报告。

通过回顾发生何种事件、采取了何种活动来解决问题以及解决程度如何等来给安全事件做出结论,从而不断进步以应对新的威胁、适应新的技术并汲取经验教训。

在安全事件发生时,被收集的安全事件数据应该在多个方面都有用。这些数据,尤其是事件总耗费时间和成本可能会被用来说明安全事件响应小组额外资金的合理性。安全事件特征研究可能会揭示出系统安全弱点和威胁,以及安全趋势的变化。这些数据也可以反馈回风险评估过程中,并最终指引着对补充安全控制的选择和实现。最后应该将所有收集的证据保存几个月或几年。

8.3 信息系统灾难恢复

8.3.1 灾难与灾难恢复

1. 灾难

灾难(disaster)是一种具有破坏性的突发事件,灾难有很多种形式,但是总体来说可分为自然灾难和人为灾难,如图 8-5 所示。自然灾难是比较典型的灾难事件,如火灾、洪水、地震、龙卷风、台风等一般会对单位的正常运营和社会的正常秩序造成影响。而人为因素引发的灾难经常也会造成大祸,最明显的影响是信息服务的中断和延迟,导致信息系统丧失技术服务能力,致使业务无法正常运营,信息系统停顿的时间越长,单位的信息化程度越高,损失就越大,如软硬件错误、通信网络中断、应用系统故障、黑客和病毒攻击等。

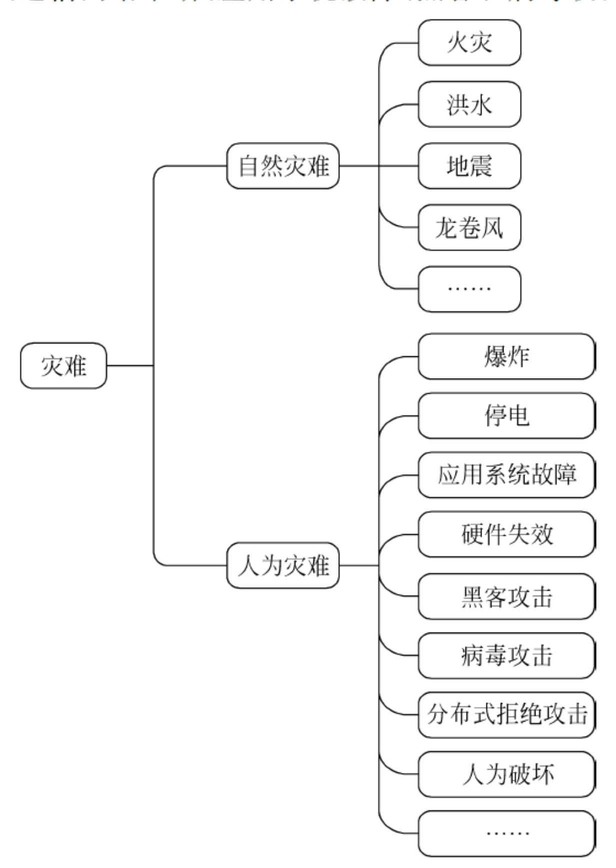


图 8-5 灾难的种类

2. 典型的灾难

AOL(美国在线),在 1996 年 8 月,由于维护工作中的人为错误造成 24 小时停机,直接损失达 300～500 万美元,股票价格相对于前一天下降 26%。

2001 年 9 月 11 日,美国世贸中心双子大厦遭受了谁也无法预料的恐怖打击,根据相关调查统计,在这两栋大楼中共有 1200 家公司,其中仅 400 家公司执行了灾难恢复计划,而大多数公司因为没有建立灾难恢复系统,数据损毁、丢失,导致业务无法恢复,最后只能宣布倒闭。

2001 年 11 月,由于对炭疽热的恐慌,临时关闭了帝国蓝十字蓝盾数据中心。

2003 年,当 AT&T 无线试图对 Siebel 客户关系管理(CRM)软件进行升级的时候,原定一个周末就能完成的项目演变为一场历时六个星期的灾难:这次 CRM 软件的升级使 AT&T 无线损失了 1 亿多美元,仅增加的用户欠款、员工加班费和承包商的佣金就高达 7500 万美元。此外,技术故障也导致该公司 2003 年第四季度的新增用户数急降 82%。

据统计,美国年均处理灾难性事件数十宗。

回过头来看一下国内发生的一些典型案例。

2003 年 7 月 4 日,首都机场离港系统因发生设备故障而瘫痪 93 分钟,无法为旅客办理登机手续,共有 71 个出港航班因此发生延误,至少 3000 名旅客无法准时登机(摘自《京华时报》、中华网)。

2005 年 5 月 1 日,黄金周第一天下午 2 点多,北京市铁路局的计算机售票系统出现临时性故障,致使全市各火车站的售票窗口、代售网点的售票工作全部处于瘫痪状态,时间长达一个多小时。而很多打算当日购票外出的乘客也因此被迫改变了离京日程,直到下午 3 点 50 分左右,瘫痪的票务网络系统才开始恢复正常,售票系统出现问题的过程中,至少有近 2000 名乘客停滞在火车站,北京站公安段为此出动了 300 余名警力在现场维持秩序,以防发生拥挤等突发事件(摘自《计算机世界》《北京青年报》、新华网)。

2005 年 6 月 9 日,北京某证券股票交易系统出现故障,迫使股民望“红”兴叹(摘自《经济观察报》《京华时报》、天极网)……

2005 年以来,国内个别银行数据运营中心的计算机系统相继发生故障,造成生产系统停机,导致部分省分行、总行营业部、机构成员的业务、交易中断(摘自《金融时报》)。

2006 年 4 月 20 日,中国银联网络长时间全面瘫痪,银行卡交易大面积停止,据估计涉及全球至少 34 万家商户,很多人不能取款转账,不能刷卡消费(摘自《金融时报》)。

众多的灾难过后,留给人们的思考就是如何减少损失、如何有效地防范风险、如何使业务不间断等。例如摩根士丹利公司、纽约交易所(NYBOT)就是很好的案例。在“9·11”事发几个小时后,摩根士丹利公司便宣布:全球营业部可以在第二天照常工作。这主要归功于该公司建立的数据备份和远程容灾系统,它们保护了公司的重要数据,在关键时刻挽救了摩根士丹利,同时也在一定程度上挽救了全球的金融行业。NYBOT 的前身 CSCF 曾经历了世贸中心车库爆炸案(1993 年),从此吸取教训而与灾难恢复服务商制订了 BCP 计划,这个计划坚持演练了 10 年。当“9·11”事件发生而导致 NYBOT 大楼被毁时,几小时后就在“长岛”开始恢复交易,这样短的时间内 NYBOT 恢复了它在异地的运营,因为它很早就制订了 BCP 计划,并在灾难发生时发挥了重要作用,NYBOT 劫后逢生的关键是 BCP 计划的策划和坚持。

经历过灾难的洗礼，一大批公司因为重要数据的毁灭而无法恢复营业，与此同时，有的公司因建立、执行了科学有效的信息系统灾难恢复机制，从而迅速恢复了业务，得到绝处逢生的机会。这些活生生的案例给人们带来了深刻的启示：重要信息系统必须构建有效的灾难恢复系统并建立业务连续性机制。

3. 灾难恢复

在《信息安全技术　信息系统灾难恢复规范(GB/T 20988—2007)》中定义的灾难恢复是指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设计的活动和流程。它的目的是减轻灾难对单位和社会带来的不良影响，保证信息系统所支持的关键业务功能在灾难发生后能及时恢复和继续运作。

为了减少灾难带来的损失和实现灾难恢复所做的事前计划和安排被称为灾难恢复规划。

灾难发生时接替生产系统运行进行数据处理和支持关键业务功能运作的场所被称为灾难备份中心。它包括备份数据处理中心、备用的工作环境、备用生活设施和技术支持及运行管理人员。

8.3.2 灾难恢复的发展

1. 国外灾难恢复发展的历史

“9·11”事件后，Globe Continuity 公司对美国、英国、澳大利亚及加拿大共 565 个公司使用灾难备份中心的情况进行了调查，发现在拥有或租用了灾难备份中心的公司中，56%使用商业化的灾难备份服务，29%使用自有的灾难备份中心，15%在商业化灾难备份服务的基础上同时拥有自己的备份设施。使用灾难备份服务外包的比例达到了 71%。

从用户的行业划分来看，灾难恢复行业面向的主要客户还是金融业。事实上，有近一半的灾难备份中心是专门为金融行业服务的。据 CPR 估计，美国灾难恢复行业的年销售额中有 45%来自金融行业。

西方发达国家重要机构都在远离主数据中心的地方拥有一个灾难恢复系统，如美国的 Wells Fargo Bank、法国的法兰西银行、新加坡的 Citibank 等。对于信息系统依赖程度较高的公司往往需要拿出总预算的 7%～15%用于灾难恢复，每月要支付 50000～100000 美元的费用，大公司甚至达到每月 100 万美元。据 Meta 预测，在全球大公司中，用于业务连续计划的投入将会持续上升，到 2007 年，这笔投入将平均达到 7%。

2. 我国信息系统灾难恢复的发展情况

20 世纪 90 年代末期，一些单位在信息化建设的同时，开始关注对数据安全的保护，进行数据的备份。2000 年，“千年虫”事件引发了国内对于信息系统灾难的第一次集体性关注，但“9·11”事件所带来的震动才真正引起了大家对灾难恢复的关注。

2003 年 9 月，为加强我国信息安全保障工作，中共中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号，以下简称《意见》)，其中明确提出要重点保障重要信息系统的安全。当前，银行、电力、民航、铁路、证券、海关、税务、保险等信息系统以及基础信息网络中的网管、计费和互联网域名注册信息系

统(以上统称重要信息系统)的安全直接影响到国民经济的正常运行和群众生活,直接关系到社会稳定和国家安全。做好灾难备份工作,是保障重要信息系统安全稳定运行的关键环节。《意见》特别强调各基础信息网络和重要信息系统的建设要充分考虑灾难发生时的抗毁性与灾难恢复能力。

2004 年 9 月份,国务院信息办公室发布《关于做好重要信息系统灾难备份工作的通知》,强调了“统筹规划、资源共享、平战结合”的灾难备份工作原则。

2005 年发布国务院信息化办公室发布《重要信息系统灾难恢复指南》,2007 年 6 月,《重要信息系统灾难恢复指南》经修订完善后正式升级为国家标准,国家质量监督检验检疫总局以国家标准的形式正式发布了《信息安全技术信息系统灾难恢复规范》(GB/T 20988—2007),该标准于 2007 年 11 月正式实施。

人民银行、银监会、保监会等出台了关于相关行业灾难恢复的政策。政府对重要行业和地方,也已经开始和正在建设相关的灾备中心。

8.4　信息系统灾难恢复工作过程

灾难恢复建设是一个系统性工程,涉及信息系统管理的使用或管理组织(以下简称组织)的组织架构、资源投入、建设与维护、流程制度变更及外部协作等多个领域,需要评估灾难恢复规划过程的风险、筹备所需资源、确定详细任务及时间表、监督和管理规划活动、跟踪和报告任务进展以及进行问题管理和变更管理。灾难恢复建设管理的目标是在资源有限的前提下根据组织的业务需求进行灾难恢复建设,减小灾难给组织带来的损失,保障业务的连续运作。

总体来说,灾难恢复规划是一个周而复始、持续改进的过程,包含灾难恢复需求的确定,灾难恢复策略的制定,灾难恢复策略的实现,灾难恢复预案的制定、落实和管理 4 个阶段。

灾难恢复主要涉及的技术和方案有数据的复制、备份和恢复,可用性方案和远程集群等,但灾难恢复不仅仅是恢复计算机系统和网络,除了技术层面的问题,还涉及风险分析、业务影响分析、策略制定和实施等方面。灾难恢复是一项系统性、多学科的专业性工作。

8.4.1　灾难恢复的需求分析

1. 方法和内容

1) 灾难恢复需求分析的实施和原则

对组织来说,在进行灾难恢复系统建设之前,首先应该对 IT 系统的现状、风险以及随之所遭受的业务影响有清醒的认知,同时兼顾预防和控制两个方面。风险分析的结果是一份有关风险分析的详细陈述报告,包括风险的精确描述、可能发生的风险、风险的范围、风险的前提或者限制因素、全面识别信息系统的灾难风险的威胁和脆弱性,以及需要采取的保障业务连续性和减少损失的措施。

根据风险分析的结果,确定业务影响分析的目标,评估业务中断影响,分析业务功能恢复条件等,得到一组防范灾难风险的指标,为下一步制定灾难恢复策略打下基础。

为了能够成功完成灾难恢复需求分析,应按照一定的要求和原则来实施。

(1) 需求分析团队的建立。分析人员要具有深厚的咨询分析经验,并且熟悉用户的业

务情况。

(2) 制定符合实际情况的项目实施流程和日程安排。

(3) 制定所要达到的目标和分析的范围,并得到用户的确认。

(4) 选择符合实际并得到用户确认的分析方法。

(5) 准确、详细地收集所有相关信息,没有遗漏。

(6) 准确地对分析要素进行赋值。

(7) 和业务人员充分地交流、沟通,深刻理解业务梳理。

同时,灾难恢复的需求分析还需要得到用户积极的支持和配合,才能确保工作的顺利完成,用户需要在如下几个阶段进行配合。

(1) 执行项目的条件。用户高度支持和配合需求分析工作:双方对需求分析的范围、目标达成一致,用户为需求分析团队提供必要的工作场所和一些基础设施。

(2) 项目执行的过程。在项目执行过程中,用户各业务部门积极配合分析团队的工作,及时提供真实的信息,以完成数据的收集。

(3) 项目结果。在项目分析结果出来后,用户积极反馈并提出相关意见和建议,协助分析。团队及时修改和完善分析结果,并最终认可需求分析结果。

2) 灾难需求分析的过程

在了解灾难恢复需求分析的原则和所需用户支持的基础上,一般会根据图 8-6 所示的过程来进行需求分析。

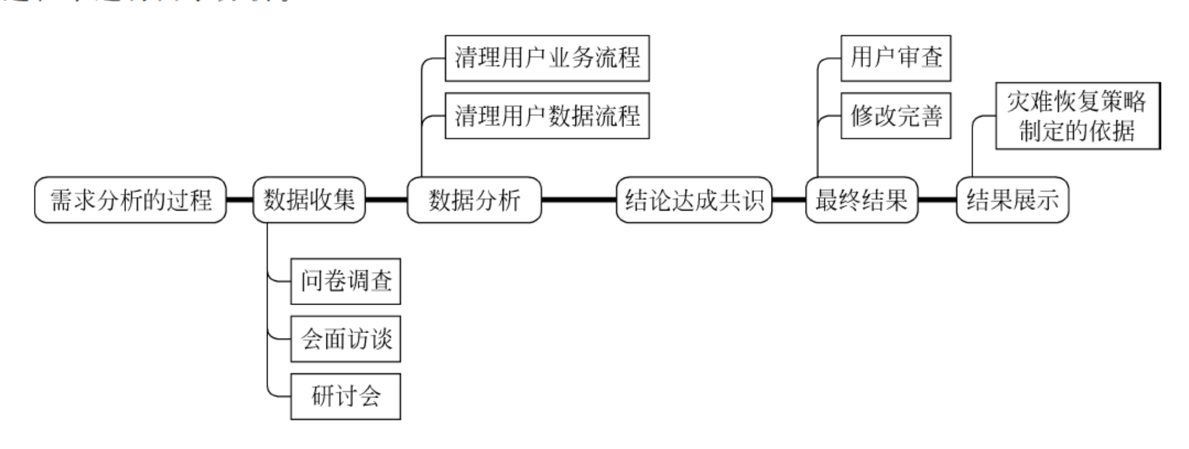


图 8-6 灾难恢复需求分析过程

(1) 数据收集阶段。为了能顺利完成信息系统灾难恢复需求分析,需求分析团队首先需要和用户进行沟通,以了解用户当前实施灾难恢复系统的背景,并对用户当前的信息系统现状和业务系统情况有初步的了解,然后根据用户的业务种类和形式等实际情况来决定需求分析的方法和思路。一般采用问卷调查、会面访谈和研讨会的方法收集数据。

(2) 数据分析阶段。根据已收集的数据进行分析,理清用户业务流程和数据流程。

(3) 结论达成共识阶段。通过数据分析,需求分析团队对分析结论达成共识。

(4) 最终结果阶段。把分析结论提交给用户审查,并根据用户的反馈意见进行修改和完善,最终得到用户的认可。

(5) 结果展示阶段。需求分析团队向用户高层汇报分析结果,并期望得到用户高层的认可,从而将结论作为下一步制定灾难恢复策略的依据。

后面的内容就将对灾难恢复需求分析所涉及的风险分析、业务影响分析和灾难恢复目

标策略制定的内容分别进行介绍。

2. 风险分析

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中规定,风险分析的主要内容包括:标识信息系统的资产价值;识别信息系统面临的自然的和人为的威胁;识别信息系统的脆弱性;分析各种威胁发生的可能性并定量或定性描述可能造成的损失;识别现有的风险防范和控制措施。通过技术和管理手段,防范或控制信息系统的风险。依据防范或控制风险的可行性和残余风险的可接受程度,确定对风险的防范和控制措施。信息系统风险评估方法可参考《信息安全技术信息安全风险评估规范(GB/T 20984—2007)》。

信息系统灾难恢复的风险分析主要根据组织的现状和业务特点,全面识别并分析影响信息系统正常运行的风险因素,分析这些因素发生的可能性。风险分析的范围主要考虑组织所在地区范围和与之在经济、业务上有紧密联系的邻近地区的交通、电信、能源及其他关键基础设施遭到严重破坏,或造成此地区的大规模人口疏散或无法联系后组织所面对的可能性风险,同时还需要考虑单位信息系统中断所造成的系统性风险。系统性风险指单位或部门因不能履行其应尽义务而导致其他机构不能开展业务,引起连锁反应,从而造成的各种社会影响和损失。

风险分析是业务影响分析与制定灾难恢复策略和预案的前期准备条件,以便在策略制定和预案制定时更具有针对性,考虑因素更为全面,规划的实施成本会更合理,从而有效地保护投资,获得更大的投资回报率。

3. 业务影响分析

1) 业务影响分析的方法和结论

风险分析完成后,得到组织一系列存在风险的业务系统范围,业务影响分析则是对这些存在风险的业务系统的功能,以及当这些功能一旦失去作用时可能造成的损失和影响进行分析,以确定组织关键业务功能及其相关性,确定支持各种业务功能的资源,明确相关信息的保密性、完整性和可用性要求,确定这些业务系统的恢复需求,为下一阶段制定灾难恢复策略提供基础和依据。

业务影响分析一般采用问卷调查、人员访谈、会议讨论等方法,从业务系统情况和业务中断影响情况两方面来收集和分析组织业务系统的相关信息,进而分析获得以下结果。

(1) 确定支持业务开展的信息系统功能。

(2) 制定不同业务系统的业务影响分析指标,从而能够确定中断对业务的损失和影响。

(3) 确定各业务系统的恢复目标和内部依赖关系。

(4) 明确各业务系统优先级和业务系统灾难恢复顺序。

(5) 明确各业务系统功能恢复的最小资源需求和恢复策略。

2) 评估中断影响

分析团队在业务影响分析时,一般采用定量和定性的方法,对各种业务功能的中断造成的影响进行评估。

定量分析是以量化方法评估业务功能的中断可能给组织带来的直接经济损失和间接经济损失。直接经济损失包括资产的损失、收入的减少、额外费用的增加、管理机构的罚款等。间接经济损失包括丧失的预期收益、丧失的商业机会、影响的市场份额。用户信息系统中断

直接经济损失分析举例如表 8-4 所示。

表 8-4　用户信息系统中断直接经济损失分析举例

业务中断损失	中断时间/小时	小于 10 万元	小于 50 万元	小于 100 万元	大于 100 万元
资产的损失	4	√			
	8		√		
	24		√		
	大于 24		√		
收入的减少	4	√			
	8		√		
	24				√
	大于 24				√
额外费用的增加	4	√			
	8	√			
	24	√			
	大于 24	√			
管理机构的罚款	4	√			
	8	√			
	24	√			
	大于 24	√			

定性分析是运用归纳与演绎、分析与综合以及抽象与概括等方法，评估业务功能的中断可能给组织带来的非经济损失，包括组织声誉、社会和政治影响、社会和政治影响、员工的信心、合作伙伴影响等。

用户信息系统中断非经济损失分析举例如表 8-5 所示。

表 8-5　用户信息系统中断非经济损失分析举例

中断无形影响	中断时间/小时	无	较小	重要	严重	非常严重
组织声誉	4			√		
	8				√	
	24					√
	大于 24					√
社会和政治影响	4			√		
	8					√
	24					√
	大于 24					√
员工的信心	4		√			
	8			√		
	24				√	
	大于 24					√
合作伙伴影响	4			√		
	8				√	
	24				√	
	大于 24				√	

4. 确定灾难恢复目标

根据前面的风险分析和业务影响分析，可以了解到组织所存在的各种风险及其程度，以及组织灾难恢复系统建设的需求、业务系统的应急需求和恢复先后顺序，完成了系统灾难恢复的各项指标。应当根据风险分析和业务影响分析的结论确定最终用户需求和灾难恢复目标，应该包括以下 5 个方面。

(1) 灾难恢复范围。根据业务影响分析确定的业务恢复范围，确定信息系统的恢复范围。

(2) 灾难恢复时间范围。根据业务影响分析的结果，确定各系统的灾难恢复时间目标(RTO)要求和恢复点目标。

(3) 灾难恢复顺序要求。根据业务影响分析中业务恢复的优先级要求，结合各系统间的资源依赖关系，制定信息系统的恢复顺序和优先级关系。

(4) 灾难恢复系统建设规划。根据灾难恢复范围、恢复时间目标和灾难恢复处理能力的要求，结合单位未来发展规划，制定灾难恢复系统建设的项目目标和时间进度目标，并按照进度要求合理规划预算投入。

(5) 根据上述灾难恢复需求分析的结果和灾难恢复目标，就可以制定灾难恢复策略，具体策略的制定方法参见 8.4.2 节。

8.4.2　灾难恢复策略的制定

1. 灾难恢复策略内容和组成

灾难恢复策略是一个组织为了达到灾难恢复的需求目标而采取的途径，它包含实现的计划、方法和可选的方案。

灾难恢复策略是基于组织对于灾难恢复需求确切了解的基础上做出的，其根本目的是为了达到在灾难恢复需求中描述的实现目标。灾难恢复策略是指导整个灾难恢复建设的纲领性文件，描述了灾难恢复需求的实现步骤和实现方法。但是，灾难恢复策略不等同于具体的技术方案，灾难恢复策略的制定是有原则性和方向性的。

可以认为灾难恢复需求是站在信息系统用户或者组织管理者的角度提出的要求和目标，而灾难恢复策略是从信息系统管理者的角度通盘考虑了信息系统现状、成本和可行性之后给出的对于实现方式、实现计划的描述，而恢复方案则是根据灾难恢复策略的要求，从实施人员的角度给出的具体执行层面的选择和描述。

2. 灾难恢复资源要素

1) 灾难恢复资源的关键要素

组织制定的信息系统灾难恢复方案能否成功实施、灾难发生时能否起到真正恢复信息系统、确保业务连续性的作用，关键要考虑信息系统灾难恢复建设的一些基本要素，例如：有没有安全的、能抵抗一定地震强度的场地；有没有考虑原先业务系统的网络的冗余；有没有制定一套完善的应急预案和灾难处理的流程；有没有建立一支能在平时对数据中心进行运行维护而在灾难发生时能应急处理和恢复系统的团队等。这些因素是灾难恢复建设必不可少的组成部分，制约着信息系统灾难恢复建设的成功与否。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中将灾难恢复资源主

要关键要素分成7类,如图8-7所示。

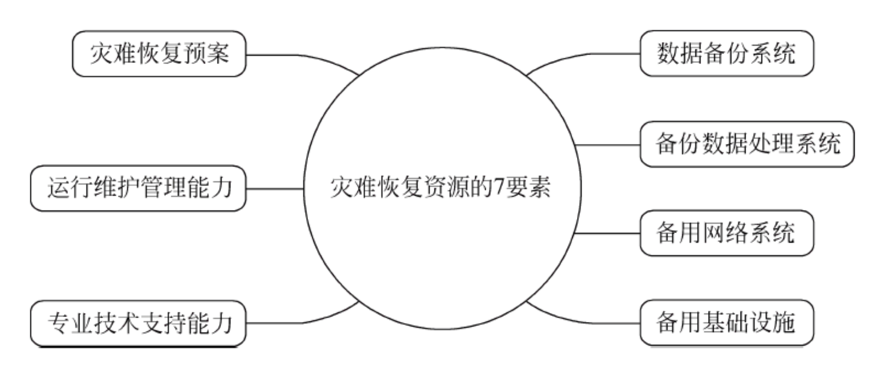


图8-7 灾难恢复资源的7要素

(1) 数据备份系统。一般由数据备份的硬件、软件和数据备份介质(以下简称介质)组成,如果是依靠电子传输的数据备份系统。还包括数据备份线路和相应的通信设备。

(2) 备用数据处理系统。指备用的计算机、外围设备和软件。

(3) 备用网络系统。最终用户用来访问备用数据处理系统的网络,包含备用网络通信设备和备用数据通信线路。

(4) 备用基础设施。灾难恢复所需的、支持灾难备份系统运行的建筑、设备和组织,包括介质的场外存放场所、备用的机房及灾难恢复工作辅助设施,以及容许灾难恢复人员连续停留的生活设施。

(5) 专业技术支持能力。对灾难恢复系统的运转提供支撑和综合保障的能力,以实现灾难恢复系统的预期目标,包括硬件、系统软件和应用软件的问题分析和处理能力、网络系统安全运行管理能力、沟通协调能力等。

(6) 运行维护管理能力。包括运行环境管理、系统管理、安全管理和变更管理等。

(7) 灾难恢复预案。定义信息系统灾难恢复过程中所需要的任务、行动、数据和资源的文件,用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

2) 灾难恢复资源的获取方式及要求

制定灾难恢复策略必须对灾难恢复资源要素的获取方式和要素进行分析和描述。灾难恢复资源各要素的需求情况如表8-6所示。

表8-6 灾难恢复资源各要素的需求情况

灾难恢复资源要素	获取方式	要求
数据备份系统	(1) 组织自行建设; (2) 租用其他机构的系统	(1) 数据备份的范围; (2) 数据备份的时间间隔; (3) 数据备份的技术及介质
备用数据处理系统	(1) 事先与厂商签订紧急供货协议; (2) 事先购买所需的数据处理设备并存放在灾难备份中心或安全的设备仓库中; (3) 利用商业化灾难备份中心或签有互惠协议的机构已有的兼容设备	(1) 数据处理能力; (2) 与主系统的兼容性要求; (3) 平时处于就绪还是运行状态

续表

灾难恢复资源要素	获取方式	要　求
备用网络系统	(1) 备用网络通信设备采用备用数据处理系统方式获取； (2) 备用数据通信线路可使用自有数据通信线路或租用公用数据通信线路	(1) 选择备用数据通信的技术和线路带宽； (2) 确定网络通信设备的功能和容量，保证灾难恢复时最终用户能以一定速率连接到备用数据处理系统
备用基础设施	(1) 由组织所有或运行； (2) 多方共建或通过互惠协议获取； (3) 租用商业化灾难备份中心的基础设施	(1) 与主中心的距离； (2) 场地和环境(如面积、温度、湿度、防火、电力和工作时间等)； (3) 运行维护和管理要求
专业技术支持能力	(1) 灾难备份中心设置专职技术支持人员； (2) 与厂商签订技术支持或服务合同； (3) 由主中心技术支持人员兼任	(1) 技术支持的组织架构； (2) 各类技术支持人员的数量和素质
运行维护管理能力	(1) 自行运行和维护； (2) 委托其他机构运行和维护	(1) 运行维护管理组织架构； (2) 人员的数量和素质； (3) 运行维护管理制度
灾难恢复预案	(1) 由组织独立完成； (2) 聘请具有相应资质的外部专家指导完成； (3) 委托具有相应资质的外部机构完成	(1) 整体要求； (2) 制定过程的要求； (3) 教育、培训和演练要求； (4) 管理要求

3. 灾难恢复等级划分和衡量指标

1) 灾难恢复等级的确定原则

实际上各单位的情况和信息系统的应用模式都有很大的不同，灾难恢复等级定义的 6 个等级对各个要素的要求也不是必须一一对应的关系，而且同一个灾难备份中心也可以同时支持不同等级的灾难恢复需求，所以灾难恢复等级的确定有两个基本原则。

(1) 要达到某个灾难恢复等级，应同时满足该等级中 7 个要素的要求。

(2) 灾难备份中心的等级等于其可以支持的灾难恢复最高等级。

简单地说，第一原则就是就低不就高，也就是说灾难恢复等级的评定是以所有 7 个要素中满足要求最低的要素对应的等级为准的。第二个原则是就高不就低，对于可以同时满足几个灾难恢复等级的灾难备份中心，按照能够满足的最高等级评定灾难备份中心的等级。

2) 灾难恢复等级的划分的国家标准和各级指标要求

为了确保灾难恢复的成功率，并且能有效降低建设成本，使得灾难恢复实现的技术手段有据可查，有必要制定一个标准，并根据用户实际信息保护的不同需求，制定不同的信息系统灾难保护等级。

信息系统灾难恢复等级的划分是根据灾难恢复资源的 7 个关键要素所达到的程度来划分的，其所能达到的程度决定了灾难恢复所能达到的等级和灾难备份中心的等级。在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中将信息系统的灾难恢复等级划分为 6 个等级，如图 8-8 所示。

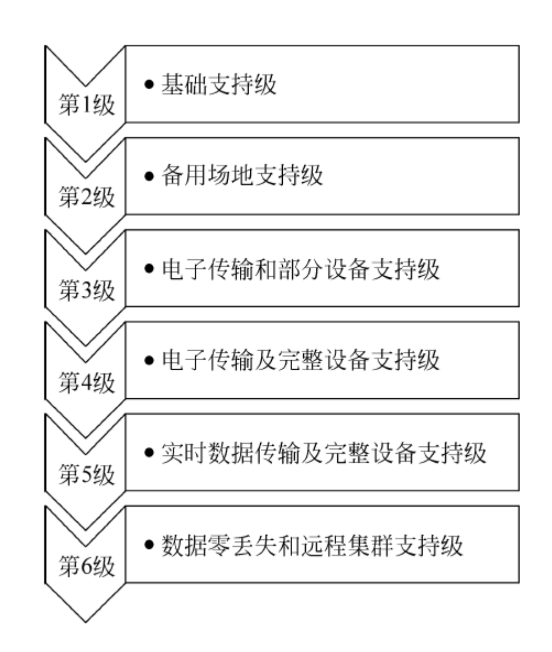


图 8-8 灾难恢复能力的六个等级

(1) 第 1 级——基础支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 1 级的指标要求如表 8-7 所示。

表 8-7 第 1 级——基本支持级的指标要求

要　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每周一次； (2) 备份介质场外存放
备用数据处理系统	—
备用网络系统	—
备用基础设施	有符合介质存放条件的场地
专业技术支持能力	—
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

注："—"表示不做要求。

(2) 第 2 级——备用场地支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 2 级的指标要求如表 8-8 所示。

表 8-8 第 2 级——备用场地支持级的指标要求

要　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每周一次； (2) 备份介质场外存放
备用数据处理系统	配备灾难恢复所需的部分数据处理设备，或灾难发生后能在预定时间内调配所需的数据处理设备到备用场地

续表

要　　素	指 标 要 求
备用网络系统	配备部分通信线路和相应的网络设备，或灾难发生后能在预定时间内调配所需的通信线路和网络设备到备用场地
备用基础设施	(1) 有符合介质存放条件的场地； (2) 有满足信息系统和关键业务功能恢复运作要求的场地
专业技术支持能力	—
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证； (3) 有备用站点管理制度； (4) 与相关厂商有符合灾难恢复时间要求的紧急供货协议； (5) 与相关运营商有符合灾难恢复时间要求的备用通信线路协议
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

注："—"表示不做要求。

(3) 第 3 级——电子传输和部分设备支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 3 级的指标要求如表 8-9 所示。

表 8-9　第 3 级——电子传输和部分设备支持级的指标要求

要　　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每天一次； (2) 备份介质场外存放； (3) 每天多次利用通信网络将关键数据定时批量传送至备用场地
备用数据处理系统	配备灾难恢复所需的部分数据处理设备
备用网络系统	配备部分通信线路和相应的网络设备
备用基础设施	(1) 有符合介质存放条件的场地； (2) 有满足信息系统和关键业务功能恢复运作要求的场地
专业技术支持能力	在灾难备份中心有专职的计算机机房运行管理人员
运行维护管理能力	(1) 按介质特性对备份数据进行定期的有效性验证； (2) 有介质存取、验证和转储管理制度； (3) 有备用计算机机房管理制度； (4) 有备用数据处理设备硬件维护管理制度； (5) 有电子传输数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

(4) 第 4 级——电子传输及完整设备支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 4 级的指标要求如表 8-10 所示。

表 8-10 第 4 级——电子传输及完整设备支持级的指标要求

要　　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每天一次； (2) 备份介质场外存放； (3) 每天多次利用通信网络将关键数据定时批量传送至备用场地
备用数据处理系统	配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态
备用网络系统	(1) 配备灾难恢复所需的通信线路； (2) 配备灾难恢复所需的网络设备，并处于就绪状态
备用基础设施	(1) 有符合介质存放条件的场地； (2) 有符合备用数据处理系统和备用网络设备运行要求的场地； (3) 有满足关键业务功能恢复运作要求的场地； (4) 以上场地应保持 7×24 小时运作
专业技术支持能力	在灾难备份中心有： (1) 7×24 小时专职计算机机房管理人员； (2) 专职数据备份技术支持人员； (3) 专职硬件、网络技术支持人员
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证； (3) 有备用计算机机房运行管理制度； (4) 有硬件和网络运行管理制度； (5) 有电子传输数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

(5) 第 5 级——实时数据传输及完整设备支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 5 级的指标要求如表 8-11 所示。

表 8-11 第 5 级——实时数据传输及完整设备支持级的指标要求

要　　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每天一次； (2) 备份介质场外存放； (3) 采用远程数据复制技术，并利用通信网络将关键数据实时复制到备用场地
备用数据处理系统	配备灾难恢复所需的全部数据处理设备，并处于就绪或运行状态
备用网络系统	(1) 配备灾难恢复所需的通信线路； (2) 配备灾难恢复所需的网络设备，并处于就绪状态； (3) 具备通信网络自动或集中切换能力
备用基础设施	(1) 有符合介质存放条件的场地； (2) 有符合备用数据处理系统和备用网络设备运行要求的场地； (3) 有满足关键业务功能恢复运作要求的场地； (4) 以上场地应保持 7×24 小时运作

续表

要　素	指 标 要 求
专业技术支持能力	在灾难备份中心 7×24 小时有以下专职人员： (1) 计算机机房管理人员； (2) 数据备份技术支持人员； (3) 硬件、网络技术支持人员
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证； (3) 有备用计算机机房运行管理制度； (4) 有硬件和网络运行管理制度； (5) 有实时数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

(6) 第 6 级——数据零丢失和远程集群支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 6 级的指标要求如表 8-12 所示。

表 8-12　第 6 级——数据零丢失和远程集群支持级的指标要求

要　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每天一次； (2) 备份介质场外存放； (3) 远程实时备份，实现数据零丢失
备用数据处理系统	(1) 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容； (2) 应用软件是“集群的”，可实时无缝切换； (3) 具备远程集群系统的实时监控和自动切换能力
备用网络系统	(1) 配备与主系统相同等级的通信线路和网络设备； (2) 备用网络处于运行状态； (3) 最终用户可通过网络同时接入主中心、备份中心
备用基础设施	(1) 有符合介质存放条件的场地； (2) 有符合备用数据处理系统和备用网络设备运行要求的场地； (3) 有满足关键业务功能恢复运作要求的场地； (4) 以上场地应保持 7×24 小时运作
专业技术支持能力	在灾难备份中心 7×24 小时有以下专职人员： (1) 计算机机房管理人员； (2) 专职数据备份技术支持人员； (3) 专职硬件、网络技术支持人员； (4) 专职操作系统、数据库和应用软件技术支持人员
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证； (3) 有备用计算机机房运行管理制度； (4) 有硬件和网络运行管理制度； (5) 有实时数据备份系统运行管理制度； (6) 有操作系统、数据库和应用软件运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

续表

要　　素	指 标 要 求
专业技术支持能力	在灾难备份中心 7×24 小时有以下专职人员： (1) 计算机机房管理人员； (2) 数据备份技术支持人员； (3) 硬件、网络技术支持人员
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证； (3) 有备用计算机机房运行管理制度； (4) 有硬件和网络运行管理制度； (5) 有实时数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

(6) 第 6 级——数据零丢失和远程集群支持级。

在《信息安全技术信息系统灾难恢复规范(GB/T 20988—2007)》中对第 6 级的指标要求如表 8-12 所示。

表 8-12　第 6 级——数据零丢失和远程集群支持级的指标要求

要　　素	指 标 要 求
数据备份系统	(1) 完全数据备份至少每天一次； (2) 备份介质场外存放； (3) 远程实时备份，实现数据零丢失
备用数据处理系统	(1) 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容； (2) 应用软件是“集群的”，可实时无缝切换； (3) 具备远程集群系统的实时监控和自动切换能力
备用网络系统	(1) 配备与主系统相同等级的通信线路和网络设备； (2) 备用网络处于运行状态； (3) 最终用户可通过网络同时接入主中心、备份中心
备用基础设施	(1) 有符合介质存放条件的场地； (2) 有符合备用数据处理系统和备用网络设备运行要求的场地； (3) 有满足关键业务功能恢复运作要求的场地； (4) 以上场地应保持 7×24 小时运作
专业技术支持能力	在灾难备份中心 7×24 小时有以下专职人员： (1) 计算机机房管理人员； (2) 专职数据备份技术支持人员； (3) 专职硬件、网络技术支持人员； (4) 专职操作系统、数据库和应用软件技术支持人员
运行维护管理能力	(1) 有介质存取、验证和转储管理制度； (2) 按介质特性对备份数据进行定期的有效性验证； (3) 有备用计算机机房运行管理制度； (4) 有硬件和网络运行管理制度； (5) 有实时数据备份系统运行管理制度； (6) 有操作系统、数据库和应用软件运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

2）灾难备份中心的基础设施的建设

灾难备份中心基础设施是灾难恢复所需的、支持灾难备份系统运行的建筑、设备，包括介质的场外存放场所、备用的机房及工作辅助设施，以及容许灾难恢复人员连续停留的生活设施。根据灾难备份中心基础设施的工作性质可以将其分为3类：第一类是工作设施；第二类是辅助设施；第三类是生活设施。在新建或选用灾难备份中心的基础设施时计算机机房应符合有关国家标准的要求，其中工作辅助设施和生活设施应符合灾难恢复目标的要求。

3）灾难备份中心的技术支持能力和管理能力

组织应根据灾难恢复策略的要求，获取对灾难备份系统的专业技术支持能力。同时，灾难备份中心应建立相应的技术支持组织，定期对技术支持人员进行技能培训。

为了达到灾难恢复目标，灾难备份中心应建立各种操作规程和管理制度，用以保证数据备份的及时性和有效性；备用数据处理系统和备用网络系统处于正常状态，并与主系统的参数保持一致；有效的应急响应、处理能力。

3. 灾难恢复预案的实现

1）灾难恢复预案的制定

灾难恢复预案是定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件，用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

在《信息安全技术信息系统灾难恢复规范（GB/T 20988—2007）》中规定灾难恢复预案的制定应遵循以下原则。

（1）完整性。灾难恢复预案（以下简称预案）应包含灾难恢复的整个过程，以及灾难恢复所需的尽可能全面的数据和资料。

（2）易用性。预案应运用易于理解的语言和图表，并适合在紧急情况下使用。

（3）明确性。预案应采用清晰的结构，对资源进行清楚的描述，工作内容和步骤应具体，每项工作应有明确的责任人。

（4）有效性。预案应尽可能满足灾难发生时进行恢复的实际需要，并保持与实际系统和人员组织的同步更新。

（5）兼容性。灾难恢复预案应与其他应急预案体系有机结合。

在灾难恢复预案制定原则的指导下，灾难恢复预案的制定流程如表8-13所示。

表8-13　灾难恢复预案的制定流程

顺序	过程步骤	主要工作及要求	形成材料
1	预案初稿的起草	参照灾难恢复预案框架，按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复能力等级的要求，结合组织其他相关的应急预案，撰写出灾难恢复预案的初稿	灾难恢复预案初稿
2	预案初稿的评审	组织应对灾难恢复预案初稿的完整性、易用性、明确性、有效性和兼容性在一定的流程下进行严格的评审	灾难恢复预案初稿评审意见
3	预案初稿的修订	根据评审意见，对预案进行修订，纠正在初稿评审过程中发现的问题和缺陷，形成预案的修订稿	灾难恢复预案修订稿

续表

顺序	过程步骤	主要工作及要求	形成材料
4	预案测试	应预先制订测试计划,在计划中说明测试的案例。测试应包含基本单元测试、关联测试和整体测试。测试的整个过程应有详细的记录,并应撰写测试报告	灾难恢复预案测试报告
5	预案初稿的完善	根据测试结果结合预案初稿评审意见,纠正在初稿评审过程和测试中发现的问题和缺陷,撰写预案审批稿	灾难恢复预案审批稿
6	预案的审核和批准	由灾难恢复领导小组对审批稿进行审核和批准,确定为预案的执行稿	灾难恢复预案的执行稿

注:灾难恢复预案框架可参考《信息系统灾难恢复规范(GB/T 20988—2007)》。

2)灾难恢复预案的教育、培训和演练

为了使相关人员了解信息系统灾难恢复的目标和流程,熟悉灾难恢复的操作规程,组织应按以下要求,组织灾难恢复预案的教育、培训和演练。

(1)在灾难恢复规划的初期就应开始灾难恢复观念的宣传教育工作。

(2)预先对培训需求进行评估,包括培训的频次和范围,开发和落实相应的培训或教育课程,保证课程内容与预案的要求相一致,事后保留培训的记录。

(3)预先制订演练计划,在计划中说明演练的场景。

(4)演练的整个过程应有详细的记录,并形成报告。

(5)每年应至少完成一次有最终用户参与的完整演练。

3)灾难恢复预案的管理

灾难恢复预案的管理包括对灾难恢复预案的保存与分发、更新管理、问题控制。经过审核和批准的灾难恢复预案,应做好保存和分发工作,包括安排专人负责保存和分发;可以以多种形式的介质备份保存在不同的安全地点;保证在生产中心以外的安全地点存放灾难安全预案或者分发给参与灾难恢复工作的所有人员;加强灾难恢复预案的版本的管理,每次修订后的所有副本统一更新,并保留一套,以备查阅,同时将已分发的旧版本按有关规定销毁。

为了保证灾难恢复预案的有效性,应对灾难恢复预案进行严格的维护和变更管理,包括业务流程的变化、信息系统的变更、人员的变更都及时反映在灾难恢复预案中;预案在测试、演练和灾难发生后实际执行时,其过程均应有详细的记录,对整个过程的效果进行评估,随后根据评估结果对预案进行相应的修订;每年应对灾难恢复预案进行至少一次评审和修订。

8.5 小　　结

本章介绍了信息安全事件的应急处理流程及灾难恢复工作过程。因为国民经济和国家安全等众多领域的关键应用日益依赖于信息技术,面对入侵和攻击事件如此频繁的网络环

境，如何保证信息系统在受攻击情况下或者出现系统异常时仍然能够正常工作，有效实现信息系统的应急响应与灾难恢复，已成为信息安全领域亟待解决的课题。

习　　题

1. 信息安全事件一般有哪几类？为每一类信息安全事件各举一个例子。
2. 信息安全事件分级的要素有哪几个方面？衡量的标准是什么？
3. 简述信息安全事件和应急响应计划之间有什么关系和联系。
4. 信息安全事件发生后应急响应要经过哪些过程？每个过程中需要完成的工作有哪些？
5. 信息安全事件处置主要有哪些阶段？各阶段又有哪些重要的控制点？
6. 列举 1～2 个信息安全事件引发的灾难，以及造成的损失。
7. 简述我国灾难恢复的发展过程，以及在灾难恢复方面的主要工作。
8. 灾难恢复规划主要包含哪些阶段？各阶段需要开展哪些工作？
9. 简述灾难恢复等级的划分及主要衡量指标。
10. 灾难恢复策略的实现要进行哪些重要的工作？如何实施？

第 9 章　信息安全标准与法律法规

本章学习目标：

- 了解信息安全相关标准。
- 了解信息安全相关法律法规。

9.1　信息安全标准

9.1.1　信息安全标准化的概述

1. 标准

国际标准化组织于 1983 年 7 月发布的 ISO 第二号指南(第四版)将标准定义为由有关各方根据科学技术成就与先进经验共同合作起草，一致同意或基本上同意的技术规范或其他公开文件，其目的在于促进最佳的公共利益，并由标准化团体批准。

我国国家标准《标准化基本术语(GB 3935.1—1983)》将标准定义为对重复性事物和概念所做的统一规定。它以科学、技术和实践经验的综合成果为基础，经有关方面协调一致，由主管机构批准，以特定形式发布，作为共同遵守的准则和依据。

2. 标准化

国家标准《标准化工作指南　第 1 部分：标准化和相关活动的通用词汇(GB/T 20000.1—2002)》对标准化的定义是为了在一定范围内获得最佳秩序，对现实问题或潜在问题制定共同使用和重复使用的条款的活动。

3. 国际标准化组织和标准

国际标准化组织(ISO)是一个全球性的非政府组织，是国际标准化领域中一个十分重要的组织，负责目前绝大部分领域(包括军工、石油、船舶等垄断行业)的标准化活动。

国际标准是由国际标准化组织通过并公开发布的标准。

4. 国家标准机构和国家标准

国家标准机构是在国家层面上承认的、有资格成为相应的国际和区域标准组织的国家成员的标准机构，如中国国家标准化管理委员会。

国家标准是国家标准机构通过并公开发布的标准。我国有 GB 字样的是强制性国家标准，有 GB/T 字样是推荐性国家标准，有 GB/Z 字样的是国家标准化指导性技术文件。

5. 信息安全标准体系的建设

信息安全标准化是国家网络安全保障体系建设的重要组成部分，在保障网络空间安全、推动网络治理体系变革方面发挥着基础性、规范性、引领性作用。信息安全标准体系是由信息安全领域内具有内在联系的标准组成的科学有机整体，是信息安全保障体系中十分重要的技术体系，是整个信息安全标准化工作的指南。只有建立了科学的信息安全标准体系，将众多的信息安全标准协调一致，才能系统化地指导行业、机构团体、产品、服务或工程项目

等,充分发挥信息安全标准的系统功能,获得良好的系统效应,取得预期的社会效益和经济效益,从而达到整体的最佳效益。

信息安全标准体系框架用以表达标准体系的构思、设想、整体规划,其主要作用是为编制信息安全标准制、修订计划提供重要依据,促进信息安全领域内的标准组成趋向科学、合理化,为信息安全保障体系建设提供支撑。

9.1.2　信息安全的国际标准

当前,世界上有 300 多个国际和区域性组织制定标准或技术规则,其中与信息安全标准化相关的国际组织也有很多,并且都有健全的信息安全标准体系,国际上影响力较大的三大信息安全标准化组织如下。

(1) 国际标准化组织(ISO)和国际电工委员会(IEC)。

(2) 国际电信联盟电信标准分局(ITU-T)。

(3) 美国国家标准和技术研究院(NIST)。

1. 国际标准 ISO 和 IEC

ISO 和 IEC 是世界范围的标准化组织,由各个国家和地区成员组成,各国的相关标准化组织都是其成员,通过各技术委员会参与相关标准的制定。

为了更好地协同规范信息技术和信息安全领域,ISO 和 IEC 联合成立了一个信息技术联合技术委员会 JTC1(信息技术标准化委员会),负责信息技术邻域的标准化工作。1990 年 4 月又成立了 JTC1 下属的安全技术分委员会 SC27,它是信息安全邻域最权威和国际认可的标准化组织,负责开展信息安全标准的研制工作。SC27 IT 安全技术分委员有 5 个工作组,分别是 WG1:要求、安全服务和指南;WG2:安全技术和机制;WG3:安全评估准则;WG4:安全控制和服务;WG5:身份管理和隐私技术。目前,安全技术分委员会 SC27 已颁布了 151 项国际标准,正在研究和制定的国际标准有 74 项,这些标准主要涉及密码算法、散列函数、数字签名、实体鉴别、安全评估、安全管理等领域,为信息安全领域的标准化工作做出了巨大的贡献。

近几年由 ISO/IEC 颁布的比较有影响力的标准有 ISO/IEC 13335 (IT 安全管理指南)、ISO/IEC 15408(安全性评估准则)、ISO/IEC 15443(IT 安全保障框架)、ISO/IEC 218279(系统安全工程能力成熟模型)和 ISO/IEC 27000 系列(信息安全管理系统,已完成 7 个部分,计划包含 20 多个子标准)。

IEC 除了和 ISO 联合成立了 JTC1 外,还在电信、电子系统、信息技术和电磁兼容等方面成立技术委员会负责安全标准研制,如 TC56(n-I 靠性)、TC74(IT 设备安全和功效)、TC77(电磁兼容)、TC 108(音频/视频)、信息技术和通信技术电子设备的安全等,并制定相关国际标准,如信息技术设备安全(IEC 60950)等。

2. 国际电信联盟电信标准 ITU-T

ITU-T 是国际电信联盟电信标准分局,是国际电信联盟管理下的专门制定电信标准的分支机构,主要负责研究通信系统安全标准,在网络与信息安全方面做出了巨大贡献。ITU-T 已经颁布了很多项网络与信息安全方面的标准,比较有影响力的安全标准主要有消息处理系统(MHS,X. 400 系列)、目录系统(X. 500 系列)、安全框架和模型(X. 800 系列)等,其中的 X. 509 标准是 PKI 的重要基础标准;X. 805 是端到端通信安全的重要标准。ITU-T 在安全标准化方面主要关注 NGN(下一代网络)安全、IPTV 安全、身份管理(IDM)、数字版权管理(DRM)、生物认证、反垃圾信息等问题。

ITU-T 下属的 SG17 组成立于 2001 年，主要负责研究通信系统信息安全标准，SG17 下设了 7 个课题组，专门从事安全标准研究，包括 Q4，通信系统安全项目组；Q5，安全体系结构和框架组；Q6，网络安全组；Q7，安全管理组；Q8，生物测定组；Q9，安全通信服务组；Q17，反垃圾邮件组。其特点是每 3 年作为一个研究周期，每个研究周期会调整工作领域和工作组的设置，在 2009—2012 年研究周期，ITU-T SG17 组共设置了 3 个工作领域（WP），分别是网络与信息安全、应用安全、身份管理和语言。3 个工作领域下设了 15 个工作组，研究范围基本涵盖了电信和信息技术领域的安全需求。在 2013—2016 年研究周期，ITU-T SG17 组将工作领域拆分成了 5 个，并根据实际标准工作需求，通过新增、裁撤等方式最终形成了 12 个工作组。ITU-T SG17 组当前的研究重点领域包括软件定义网络、云计算、物联网、生物特征识别、个人信息保护等。

3. 美国信息安全管理标准体系

美国国家标准技术委员会（National Institute of Standards and Technology，NIST）成立于 1901 年，隶属于美国商务部技术司，主要负责为美国政府和商业机构提供信息安全管理相关的标准规范。NIST 信息技术实验室下设的计算机安全研究室（Computer Security Division，CSD）和应用网络空间安全研究室（Applied Cyber-security Division，ACD）是 NIST 信息安全标准的主要制定部门。

NIST 发布的信息安全标准和文件类型包括联邦信息处理标准系列（FIPs）、特别出版物系列（special Publication，SP）、内部报告系列（IRs）和信息技术实验室安全快报系列（ITLs）等。联邦信息处理标准大部分为强制标准，要求大多数的联邦政府部门按照标准中的规定执行。截至 2016 年 5 月，有效的 FIPS 共 9 项，涉及密码算法、联邦政府信息系统保护两个方面。SP800 系列是 NIST 在信息技术安全方面的特别出版物，起始于 1990 年。SP800 系列均属于技术指南文件，对联邦政府部门不具有强制性，只是提供一种供参考的方法或经验，涉及的内容包括系统和应用安全、安全基础组件和机制、安全测试与评估等。

NIST 近年来在云计算和大数据技术标准化研究方面贡献突出，其发布的云计算、大数据参考架构、公有云中的安全与隐私指南等标准对相关国际标准化工作影响深刻。NIST 同样注重标准体系梳理工作，在云计算和大数据领域分别发布了标准路线图，分析相关标准现状及存在问题，提出当前标准缺口，并根据迫切程度提出 NIST 标准研究优先级的建议。

9.1.3 信息安全国内标准

1. 我国的信息安全标准化组织

我国于 1984 年成立了数据加密技术分委员，后来改为信息技术安全分技术委员会，2002 年 4 月，为加强信息安全标准的协调工作，国家标准委员会决定成立全国信息安全标准化技术委员会（简称信安标委，编号 TC260），它是国家标准化管理委员会的直属标委会，从事全国信息安全标准化工作，统一协调和申报信息安全国家标准年度计划项目，组织国家标准的送审、报批、宣贯等工作，对口 ISO/IEC JTC1 SC27，秘书处设在中国电子技术标准化研究所，委员会由 30 多个部门和单位的 49 名领导和专家组成。

全国信息安全标准化技术委员会以工作组为主体开展信息安全标准的研究制定工作，工作组由国内信息安全技术领域的有关部门、研究机构、企事业单位及高等院校等代表组成，是信息安全标准研制的技术力量，已正式成立了 7 个工作组，分别是 WG1（信息安全标准体系与协调工作组，下设一个可信计算工作小组）、WG2（涉密信息系统安全保密标准工作组）、WG3（密码技术标准工作组）、WG4（鉴别与授权工作组）、WG5（信息安全评估工作

组，下设一个生物特征识别小组）、WG6（通信安全标准工作组）以及 WG7（信息安全管理工作组）。各小组工作职责和范围如表 9-1 所示。

表 9-1　信安标委工作组工作职责和范围

工作小组名称	工 作 职 责	备　注
信息安全标准体系与协调工作组（WG1）	（1）研究信息安全标准体系； （2）跟踪国际标准发展动态； （3）研究信息安全标准需求； （4）研究并提出新工作项目及设立新工作组的建议； （5）协调各工作组项目	下设一个可信计算工作小组
涉密信息系统安全保密标准工作组（WG2）	（1）研究提出涉密信息系统安全保密标准体系； （2）制定和修订涉密信息系统安全保密标准	
密码技术标准工作组（WG3）	（1）研究提出商用密码技术标准体系； （2）研究制定商用密码算法、商用密码模块和商用密钥管理等相关标准	
鉴别与授权工作组（WG4）	（1）研制鉴别与授权标准体系； （2）调研国内相关标准需求； （3）研究制定鉴别与授权标准	
信息安全评估工作组（WG5）	（1）调研测评标准现状与发展趋势； （2）研究我国统一测评标准体系的思路和框架，提出测评标准体系； （3）研究制定急需的测评标准	下设一个生物特征识别小组
通信安全标准工作组（WG6）	（1）调研通信安全标准现状与发展趋势； （2）研究提出通信安全标准体系； （3）研究制定急需的通信安全标准	
信息安全管理工作组（WG7）	（1）研究信息安全管理动态，调研国内信息安全管理标准需求； （2）研究提出信息安全管理标准体系； （3）制定信息安全管理相关标准	

国标委高新函[2004]1 号文规定，自 2004 年 1 月起，各有关部门在申报信息安全国家标准计划项目时，必须经全国信息安全标准化技术委员会提出工作意见，协调一致后由全国信息安全标准化技术委员会组织申报；在国家标准制定过程中，标准工作组或主要起草单位要与全国信息安全标准化技术委员会积极合作，并由全国信息安全标准化技术委员会完成国家标准送审、报批工作。

2. 我国的信息安全标准化体系

近年来，我国非常重视信息安全标准建设工作，基本形成了国家和行业层面的相对完整的信息安全标准体系，目前国内涉及信息安全标准化工作的组织机构主要是全国信息技术安全标准化技术委员会和中国通信标准化协会。

全国信息技术安全标准化技术委员会本着“科学、合理、系统、适用”的原则，总结各工作组对本领域标准体系的研究成果，同时在跟踪分析了国际信息安全标准的发展动态和国内信息安全标准需求的基础上，提出了我国信息安全标准体系框架和标准体系表，形成我国信

息安全标准体系，如图 9-1 所示。该体系是指导我国信息安全标准制定和修订工作开展时的指导性技术文件，它将随着信息安全技术的发展而不断完善。

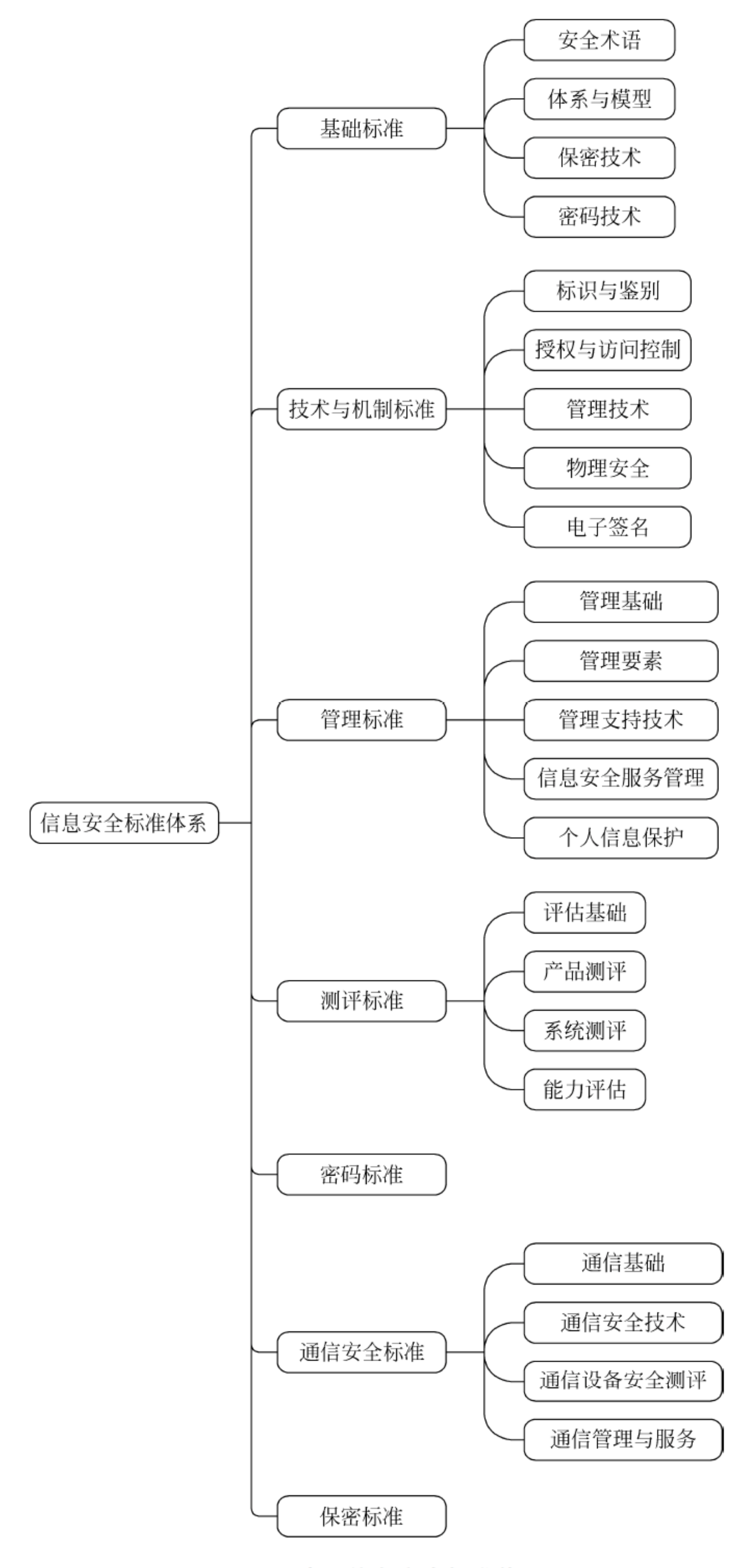


图 9-1 我国信息安全标准体系

3. 我国的信息安全标准

我国的信息安全标准化方面，截至 2013 年底，共组织申报信息安全国家标准 290 项，其中 249 项已批准列入国家标准制修订计划，截至 2013 年底正式发布国家标准 140 项，其中采用国际标准的有 35 项，参考国外先进标准制定的有 18 项，我国自主制定的标准有 87 项，这些标准主要涉及信息安全技术与机制、信息安全管理、信息安全评估以及保密、密码和通信安全等领域。这些标准为我国信息安全等级保护制度实施和网络信任体系建设提供了基础标准支撑；为信息安全应急处理和《电子签名法》的顺利实施提供了重要技术支持；为信息安全产品测评认证提供了重要依据，同时也为电子政务等国家重大工程建设提供必要标准服务。

随着信息安全技术的不断发展和信息安全形势的不断变化，不但信息安全标准数量在不断增加，而且许多标准的版本也在不断更新。

为推动我国信息安全等级保护工作，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制定了信息安全等级保护工作需要的一系列标准，为开展等级保护工作提供了标准保障。这些标准可以分为基础类、应用类、产品类和其他类，这些标准包括在国家标准(GB)和公共安全行业标准(GA)中，表 9-2 列举了我国信息系统安全等级保护的相关标准。本书后续内容将主要介绍一些和计算机信息系统安全等级保护相关的一些标准。

表 9-2　信息系统安全等级保护相关标准

<table>
<tr><th>标准类型</th><th>子类型</th><th>标准名称</th><th>备注</th></tr>
<tr><td>基础类标准</td><td>—</td><td>计算机信息系统安全保护等级划分准则(GB 17859—1999)</td><td>▲</td></tr>
<tr><td rowspan="15">应用类标准</td><td>信息系统定级</td><td>信息系统安全保护等级定级指南(GB/T 22240—2008)</td><td>▲</td></tr>
<tr><td>等级保护实施</td><td>信息系统安全等级保护实施指南(信安字[2007]10)</td><td>▲</td></tr>
<tr><td rowspan="10">信息系统安全建设</td><td>信息系统安全等级保护基本要求(GB/T 22239—2008)</td><td>▲</td></tr>
<tr><td>信息系统通用安全技术要求(GB/T 20271—2006)</td><td></td></tr>
<tr><td>信息系统等级保护安全设计技术要求(GB/T 24856—2009)</td><td>▲</td></tr>
<tr><td>信息系统安全管理要求(GB/T 20269—2006)</td><td></td></tr>
<tr><td>信息系统安全工程管理要求(GB/T 20282—2006)</td><td></td></tr>
<tr><td>信息系统物理安全技术要求(GB/T 21052—2007)</td><td></td></tr>
<tr><td>网络基础安全技术要求(GB/T 20270—2006)</td><td></td></tr>
<tr><td>信息系统安全等级保护体系框架(GA/T 708—2007)</td><td></td></tr>
<tr><td>信息系统安全等级保护基本模型(GA/T 709—2007)</td><td></td></tr>
<tr><td>信息系统安全等级保护基本配置(GA/T 710—2007)</td><td></td></tr>
<tr><td rowspan="3">等级测评</td><td>信息系统安全等级保护测评要求(GB/T 28448—2012)</td><td>▲</td></tr>
<tr><td>信息系统安全等级保护测评过程指南(GB/T 28449—2012)</td><td>▲</td></tr>
<tr><td>信息系统安全管理测评(GA/T 713—2007)</td><td></td></tr>
<tr><td rowspan="4">产品类标准</td><td rowspan="2">操作系统</td><td>操作系统安全技术要求(GB/T 20272—2006)</td><td></td></tr>
<tr><td>操作系统安全评估准则(GB/T 20008—2005)</td><td></td></tr>
<tr><td rowspan="2">数据库</td><td>数据库管理系统安全技术要求(GB/T 20273—2006)</td><td></td></tr>
<tr><td>数据库管理系统安全评估准则(GB/T 20009—2005)</td><td></td></tr>
</table>

续表

标准类型	子类型	标准名称	备注
	网络	网络端设备隔离部件技术要求(GB/T 20279—2006)	
		网络端设备隔离部件测试评价方法(GB/T 20277—2006)	
		网络脆弱性扫描产品技术要求(GB/T 20278—2006)	
		网络脆弱性扫描产品测试评价方法(GB/T 20280—2006)	
		网络交换机安全技术要求(GA/T 684—2007)	
		虚拟专用网安全技术要求(GA/T 686—2007)	
	PKI	公钥基础设施安全技术要求(GA/T 687—2007)	
		PKI 系统安全等级保护技术要求(GB/T 21053—2007)	
	网关	网关安全技术要求(GA/T 681—2007)	
	服务器	服务器安全技术要求(GB/T 21028—2007)	
	入侵检测	入侵检测系统技术要求和检测方法(GB/T 20275—2006)	
		计算机网络入侵分级要求(GA/T 700—2007)	
	防火墙	防火墙安全技术要求(GA/T 683—2007)	
		防火墙技术测评方法(报批稿)	
		信息系统安全等级保护防火墙安全配置指南(报批稿)	
		防火墙技术要求和测评方法(GB/T 20281—2006)	
		包过滤防火墙评估准则(GB/T 20010—2005)	
	路由器	路由器安全技术要求(GB/T 18018—2007)	
		路由器安全评估准则(GB/T 20011—2005)	
		路由器安全测评要求(GA/T 682—2007)	
	交换机	网络交换机安全技术要求(GB/T 21050—2007)	
		交换机安全测评要求(GA/T 685—2007)	
	其他产品	终端计算机系统安全等级技术要求(GA/T 671—2006)	
		终端计算机系统测评方法(GA/T 671—2006)	
		审计产品技术要求和测评方法(GB/T 20945—2006)	
		虹膜特征识别技术要求(GB/T 20979—2007)	
		虚拟专网安全技术要求(GA/T 686—2007)	
		应用软件系统安全等级保护通用技术指南(GA/T 711—2007)	
		应用软件系统安全等级保护通用测试指南(GA/T 712—2007)	
其他类标准	风险评估	信息安全风险评估规范(GB/T 20984—2007)	
	事件管理	信息安全事件管理指南(GB/Z 20985—2007)	
		信息安全事件分类分级指南(GB/Z 20986—2007)	
		信息系统灾难恢复规范(GB/T 20988—2007)	

以上标注“▲”的将在本书后面的章节中进行详细的介绍,应用中如果需要参考其他标准的读者请自行查找相关资料进行学习。国家信息安全标准项目管理与服务平台网址为 http://www.tc260.org.cn。

9.1.4 计算机信息系统安全保护等级划分准则(GB 17859—1999)

《计算机信息系统安全保护等级划分准则(GB 17859—1999)》是强制性国家标准,是其他各标准制定的基础,为计算机信息系统安全法规的制定和执法部门的监督检查提供依据,

为安全产品的研制提供技术支持，同时为安全系统的建设和管理提供技术指导。该标准的制定参考了美国的可信计算机系统评估准则(DoD 5200.28-STD)和可信计算机网络系统说明(NCSC-TG-005)。

1. 安全保护的 5 个等级及适用范围

GB 17859—1999 标准规定了计算机信息系统安全保护能力的 5 个等级。

(1) 第 1 级：用户自主保护级。

(2) 第 2 级：系统审计保护级。

(3) 第 3 级：安全标记保护级。

(4) 第 4 级：结构化保护级。

(5) 第 5 级：访问验证保护级。

GB 17859—1999 标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高逐渐增强。

2. GB 17859—1999 标准涉及术语的定义

1) 计算机信息系统

计算机信息系统(computer information system)是由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2) 计算机信息系统可信计算基

计算机信息系统可信计算基(trusted computing base of computer information system)是计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

3) 客体

客体(object)指信息的载体。

4) 主体

主体(subject)指引起信息在客体之间流动的人、进程或设备等。

5) 敏感标记

敏感标记(sensitivity label)表示客体安全级别并描述客体数据敏感性的一组信息。可信计算基中把敏感标记作为强制访问控制决策的依据。

6) 安全策略

安全策略指(security policy)有关管理、保护和发布敏感信息的法律、规定和实施细则。

7) 信道

通道指(channel)系统内的信息传输路径。

8) 隐蔽信道

隐蔽信道(covert channel)指允许进程以危害系统安全策略的方式传输信息的通信信道。

9) 访问监控器

监控主体和客体之间授权访问关系的部件称为访问监控器(reference monitor)。

3. 安全保护5个等级的划分准则

1) 第1级　用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据,使用户具备自主安全保护的能力。它具有多种形式的控制能力,对用户实施访问控制,即为用户提供可行的手段,保护用户和用户组信息,避免其他用户对数据的非法读写与破坏。

第1级的计算机信息系统应具备如下安全保护能力。

(1) 自主访问控制。计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享;阻止非授权用户读取敏感信息。

(2) 身份鉴别。计算机信息系统可信计算基初始执行时,首先要求用户标识自己的身份,并使用保护机制(例如口令)来鉴别用户的身份,阻止非授权用户访问用户身份鉴别数据。

(3) 数据完整性。计算机信息系统可信计算基通过自主完整性策略,阻止非授权用户修改或破坏敏感信息。

2) 第2级　系统审计保护级

与用户自主保护级相比,本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制,它通过登录规程、审计安全性相关事件和隔离资源,使用户对自己的行为负责。

第2级的计算机信息系统应具备如下安全保护能力。

(1) 自主访问控制。计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享;阻止非授权用户读取敏感信息,并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式,阻止非授权用户访问客体。访问控制的粒度是单个用户,没有存取权的用户只允许由授权用户指定对客体的访问权。

(2) 身份鉴别。信息系统可信计算基初始执行时,首先要求用户标识自己的身份,并使用保护机制(例如口令)来鉴别用户的身份;阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识,计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(3) 客体重用。在计算机信息系统可信计算基的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

(4) 审计。计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录,并阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件:使用身份鉴别机制;将客体引入用户地址空间(例如打开文件、程序初始化),删除客体;由操作员、系统管理员或(和)系统安全管理员实施的动作,以及其他与系统安全有关的事件。对于每一事件,其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件,审计记录包含请求的来源(例如终端标识符)。对于客体引入用户地址空间的事件及客体删除事件,审计记录包含客体名。

对不能由计算机信息系统可信计算基独立分辨的审计事件,审计机制提供审计记录接

口,可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。

(5) 数据完整性。计算机信息系统可信计算基通过自主完整性策略,阻止非授权用户修改或破坏敏感信息。

3) 第 3 级　安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外,还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述,具有准确地标记输出信息的能力,消除通过测试发现的任何错误。

第 3 级的计算机信息系统应具备如下安全保护能力。

(1) 自主访问控制。计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享;阻止非授权用户读取敏感信息,并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式,阻止非授权用户访问客体;访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权,阻止非授权用户读取敏感信息。

(2) 强制访问控制。计算机信息系统可信计算基对所有主体及其所控制的客体(例如进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基控制的所有主体对客体的访问应满足:仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别,主体才能读客体;仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含于客体安全级中的非等级类别,主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据,鉴别用户的身份,并保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

(3) 标记。计算机信息系统可信计算基应维护与主体及其控制的存储客体(例如进程、文件、段、设备)相关的敏感标记,这些标记是实施强制访问的基础。为了输入未加安全标记的数据,计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别,且可由计算机信息系统可信计算基审计。

(4) 身份鉴别。计算机信息系统可信计算基初始执行时,首先要求用户标识自己的身份。计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据鉴别用户身份,并使用保护机制(例如口令)来鉴别用户的身份;阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识,计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(5) 客体重用。在计算机信息系统可信计算基的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

(6) 审计。计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录,并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间(例如打开文件、程序初始化)；删除客体；由操作员、系统管理员或(和)系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源(例如终端标识符)；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。此外，计算机信息系统可信计算基具有审计、更改可读输出记号的能力。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。

(7) 数据完整性。计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

4) 第 4 级 结构化保护级

本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第 3 级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审，加强了鉴别机制；支持系统管理员和操作员的职能，提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

第 4 级的计算机信息系统应具备如下安全保护能力。

(1) 自主访问控制。计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如访问控制表)允许命名用户和(或)以用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息并控制访问权限扩散。

自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。

(2) 强制访问控制。计算机信息系统可信计算基对外部主体能够直接或间接访问的所有资源(例如主体、存储客体和输入输出资源)实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基外部的所有主体对客体的直接或间接的访问应满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体；仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含于客体安全级中的非等级类别，主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

(3) 标记。计算机信息系统可信计算基维护与可被外部主体直接或间接访问到的计算机信息系统资源(例如主体、存储客体、只读存储器)相关的敏感标记，这些标记是实施强制

访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。

(4) 身份鉴别。计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据，鉴别用户身份，并使用保护机制(例如口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(5) 客体重用。在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

(6) 审计。计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间(例如打开文件、程序初始化)；删除客体；由操作员、系统管理员或(和)系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源(例如终端标识符)；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。此外，计算机信息系统可信计算基具有审计、更改可读输出记号的能力。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

(7) 数据完整性。计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

(8) 隐蔽信道分析。系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

(9) 可信路径。对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径，该路径上的通信只能由该用户初始化。

5) 第5级　访问验证保护级

本级的计算机信息系统可信计算基满足访问监控器需求，访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最低程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

第5级的计算机信息系统应具备如下安全保护能力。

(1) 自主访问控制。计算机信息系统可信计算基定义并控制系统中命名用户对命名客

体的访问,实施机制(例如访问控制表)允许命名用户和(或)以用户组的身份规定并控制客体的共享;阻止非授权用户读取敏感信息,并控制访问权限扩散。

自主访问控制机制根据用户指定方式或默认方式,阻止非授权用户访问客体。访问控制的粒度是单个用户。访问控制能够为每个命名客体指定命名用户和用户组,并规定其对客体的访问模式。没有存取权的用户只允许由授权用户指定对客体的访问权。

(2) 强制访问控制。计算机信息系统可信计算基对外部主体能够直接或间接访问的所有资源(例如主体、存储客体和输入输出资源)实施强制访问控制,为这些主体及客体指定敏感标记这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基外部的所有主体对客体的直接或间接的访问应满足:仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别,主体才能读客体,仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含于客体安全级中的非等级类别,主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据,鉴别用户的身份,保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

(3) 标记。计算机信息系统可信计算基维护与可被外部主体直接或间接访问到的计算机信息系统源(例如主体、存储客体、只读存储器)相关的敏感标记,这些标记是实施强制访问的基础。为了输入未加安全标记的数据,计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别,且可由计算机信息系统可信计算基审计。

(4) 身份鉴别。计算机信息系统可信计算基初始执行时,首先要求用户标识自己的身份。计算机信系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据鉴别用户身份,并使用保护机制(例如口令)来鉴别用户的身份;阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识,计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(5) 客体重用。在计算机信息系统可信计算基的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

(6) 审计。计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录,并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件:使用身份鉴别机制;将客体引入用户地址空间(例如打开文件、程序初始化);删除客体;由操作员、系统管理员或(和)系统安全管理员实施的动作,以及其他与系统安全有关的事件。对于每一事件,其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件,审计记录包含请求的来源(例如终端标识符);对于客体引入用户地址空间的事件及客体删除事件,审计记录包含客体名及客体的安全级别。此外,计算机信息系统可信计算基具有审计、更改可读输出记号的能力。

对不能由计算机信息系统可信计算基独立分辨的审计事件,审计机制提供审计记录接口,可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的

审计记录。计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

计算机信息系统可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出警报，并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价终止它们。

(7) 数据完整性。计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

(8) 隐蔽信道分析。系统开发者应彻底搜索隐蔽信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

(9) 可信路径。当连接用户时(如注册、更改主体安全级)，计算机信息系统可信计算基提供它与用户之间的可信通信路径。可信路径上的通信只能由该用户或计算机信息系统可信计算基激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分。

(10) 可信恢复。计算机信息系统可信计算基提供过程和机制，保证计算机信息系统失效或中断后可以进行不损害任何安全保护性能的恢复。

4. 5 个安全等级保护能力的比较

根据对 GB 17859—1999 标准的介绍，可以看到不同等级的计算机系统具有不同的安全保护能力，第 1 到第 5 级的安全保护等级是在逐步增高的，对应的安全保护的能力也在逐渐增强。5 个安全等级保护能力综合比较如表 9-3 所示。

表 9-3　安全等级保护能力综合比较一览表

保护能力项目	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
自主访问控制	●	●	●	●	●
强制访问控制			●	●	●
标记			●	●	●
身份鉴别	●	●	●	●	●
客体重用		●	●	●	●
审计		●	●	●	●
数据完整性	●	●	●	●	●
隐蔽信道分析				●	●
可信路径				●	●
可信恢复					●

9.1.5　信息安全等级保护其他相关标准

1. 信息安全等级保护相关标准概述

多年来，在有关部门的支持下，在国内有关专家、企业的共同努力下，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制定了信息安全等级保护工作需要的一系列标准(具体标准见表 9-2)，各标准在信息安全等级保护建设的各环节中都发挥了很重要的指导作用，形成了比较完整的信息安全等级保护标准体系，如图 9-2 所示。

《计算机信息系统安全保护等级划分准则(GB 17859—1999)》(以下简称《等级划分准

则》)是强制性国家标准,是其他各信息安全等级保护标准制定的基础,标准的具体内容已在9.1.4节做了详细介绍。

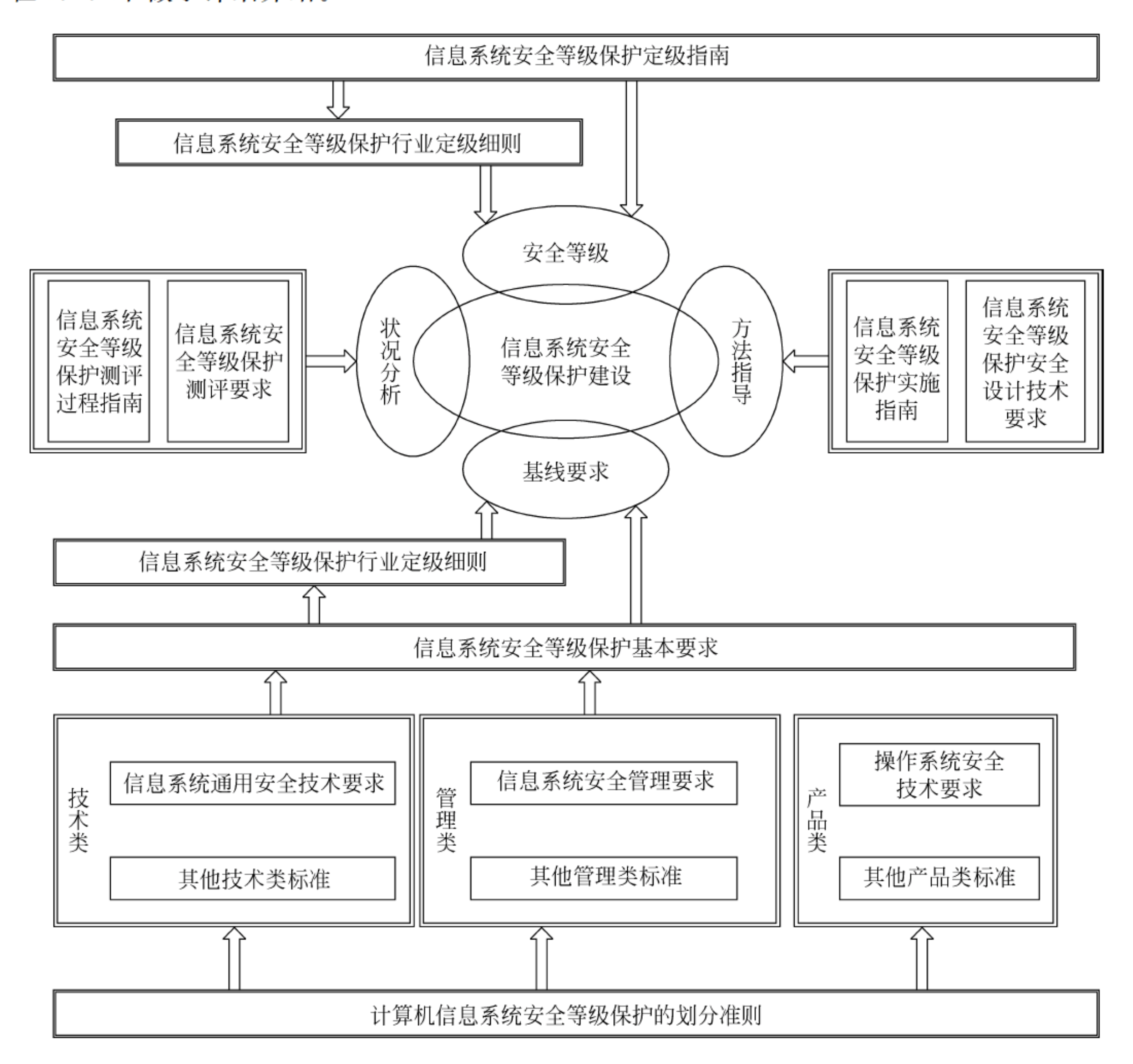


图 9-2 信息安全等级保护标准在各工作环节的作用

《信息系统安全保护等级定级指南(GB/T 22240—2008)》(以下简称《定级指南》)规定了定级的依据、对象、流程和方法以及等级变更等内容,同各行业发布的定级实施细则共同用于指导开展信息系统定级工作。

《信息系统安全等级保护基本要求(GB/T 22239—2008)》(以下简称《基本要求》)是在《等级划分准则》以及各技术类标准、管理类标准和产品类标准(所含标准见表 9-2)基础上制定的,给出了各级信息系统应当具备的安全防护能力,并从技术和管理两个方面提出了相应的措施,是信息系统进行建设整改的安全需求。

《信息系统安全等级保护实施指南(信安字[2007]10)》(以下简称《实施指南》)和《信息系统等级保护安全设计技术要求(GB/T 24856—2009)》(以下简称《技术要求》)构成了指导信息系统安全建设整改的方法指导类标准。《实施指南》阐述了在系统建设、运维和废止等各个生命周期阶段中如何按照信息安全等级保护政策、标准要求实施等级保护工作;《技术

要求》提出了信息系统等级保护安全设计的技术要求，包括安全计算环境、安全区域边界、安全通信网络、安全管理中心等各方面的要求。

《信息系统安全等级保护测评要求 GB/T 28448—2012》（以下简称《测评要求》）和《信息系统安全等级保护测评过程指南 GB/T 28449—2012》（以下简称《测评指南》）构成了指导开展等级测评的标准规范。《测评要求》阐述了等级测评的原则、测评内容、测评强度、单元测评、整体测评、测评结论的产生方法等内容；《测评指南》阐述了信息系统等级测评的过程，包括测评准备、方案编制、现场测评、分析与报告编制等各个活动的工作任务、分析方法和工作结果等。

2. 信息系统安全等级保护定级

《定级指南》依据等级保护相关管理文件，从信息系统所承载的业务在国家安全、经济建设、社会生活中的重要作用和业务对信息系统的依赖程度这两方面，提出确定信息系统安全保护等级的方法。

在《定级指南》中明确了等级保护的对象是信息安全等级保护工作直接作用的具体信息和信息系统。客体是受法律保护的、等级保护对象受到破坏时所侵害的社会关系，如国家安全、社会秩序、公共利益以及公民、法人或其他组织的合法权益。系统服务是信息系统为支持其所承载业务而提供的程序化过程。

1）信息系统安全保护等级

在《定级指南》中明确了根据等级保护相关管理文件，信息系统的安全保护等级分为以下 5 级。

第 1 级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第 2 级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第 3 级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第 4 级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第 5 级，信息系统受到破坏后，会对国家安全造成特别严重损害。

2）定级要素与信息系统安全保护等级

《定级指南》中明确了信息系统的安全保护等级的两个定级要素是等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。《定级指南》中还指明了各定级要素所包含的内容。定级要素与信息系统安全保护等级的关系如表 9-4 所示。

表 9-4　定级要素与信息系统安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第 1 级	第 2 级	第 3 级
社会秩序、公共利益	第 2 级	第 3 级	第 4 级
国家安全	第 3 级	第 4 级	第 5 级

3）定级方法和流程

《定级指南》还给出了确定等级一般流程，流程一共涉及8个步骤，具体步骤和流程如图9-3所示，流程中的每个步骤如何进行，请读者具体参考《信息系统安全保护等级定级指南(GB/T 22240—2008)》。

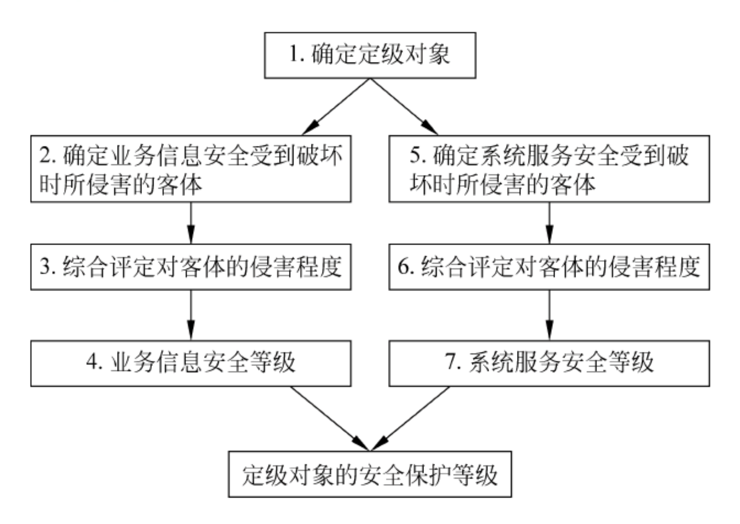


图9-3 信息安全等级保护定级的一般流程

3. 信息系统安全等级保护基本要求

《信息系统安全等级保护基本要求(GB/T 22239—2008)》(以下简称《基本要求》)根据现有技术的发展水平，提出和规定了不同安全保护等级信息系统的最低保护要求，即基本安全要求，基本安全要求包括基本技术要求和基本管理要求，适用于指导不同安全保护等级信息系统的安全建设和监督管理。

重点行业可以按照《基本要求》等国家标准，结合行业特点，在公安部等有关部门指导下，确定《基本要求》的具体指标，在不低于《基本要求》的情况下，结合系统安全保护的特殊需求，制定行业标准规范或细则。

1）信息系统安全保护等级概述

《基本要求》定义了安全保护能力是系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复之前状态等的程度。信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为5级，这5级的划分准则已在《划分准则》中进行了定义。在《基本要求》中对不同等级的信息系统应具备的基本安全保护能力明确如下。

(1) 第1级安全保护能力。能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

(2) 第2级安全保护能力。能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

(3) 第3级安全保护能力。能够在统一安全策略下防护系统免受来自外部有组织的团

体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

(4) 第 4 级安全保护能力。能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

(5) 第 5 级安全保护能力(略)。

信息系统安全等级保护应依据信息系统的安全保护等级情况保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统要求具有不同的安全保护能力。

2) 信息安全等级保护的基本安全要求

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类，是确保信息系统安全不可分割的两个部分。

基本技术要求从物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复几个层面提出，技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确配置其安全功能来实现。

基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出。管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。图 9-4 所示表示了基本安全要求两个类的各个层面。

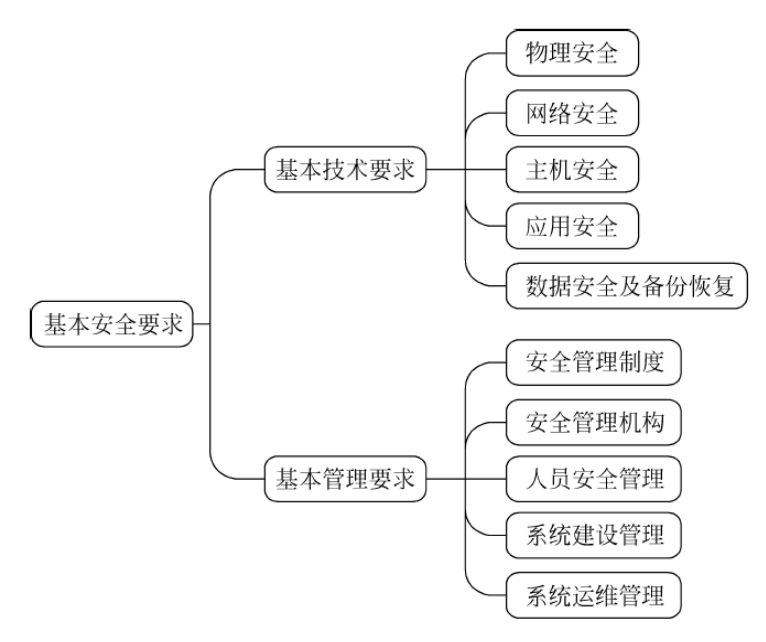


图 9-4　信息安全等级保护基本安全要求两类的各层面

《基本要求》明确了基本安全要求从各个层面或方面提出了系统的每个组件应该满足的安全要求，信息系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证，除了保证系统的每个组件满足基本安全要求外，还要考虑组件之间的相互关系，来保证信息系统

的整体安全保护能力。关于信息系统整体安全保护能力的说明请读者参阅《基本要求》附录 A。

对于涉及国家秘密的信息系统，应按照国家保密工作部门的相关规定和标准进行保护。对于涉及密码的使用和管理，应按照国家密码管理的相关规定和标准实施。

根据保护侧重点的不同，《基本要求》对技术类安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄露、破坏和免受未授权地修改的信息安全类要求（简记为 S）；保护系统连续正常地运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；通用安全保护类要求（简记为 G）。

《基本要求》对基本安全要求使用了标记，其中的字母表示安全要求的类型，数字表示适用的安全保护等级。关于各类安全要求的选择和使用请读者参阅《基本要求》附录 B。

3）基本要求的特点

《基本要求》从第 5～9 章分别针对不同安全保护等级信息系统应该具有的基本安全保护能力提出了对应的基本安全要求，图 9-5 所示是描述某级别系统等级保护能力的结构。

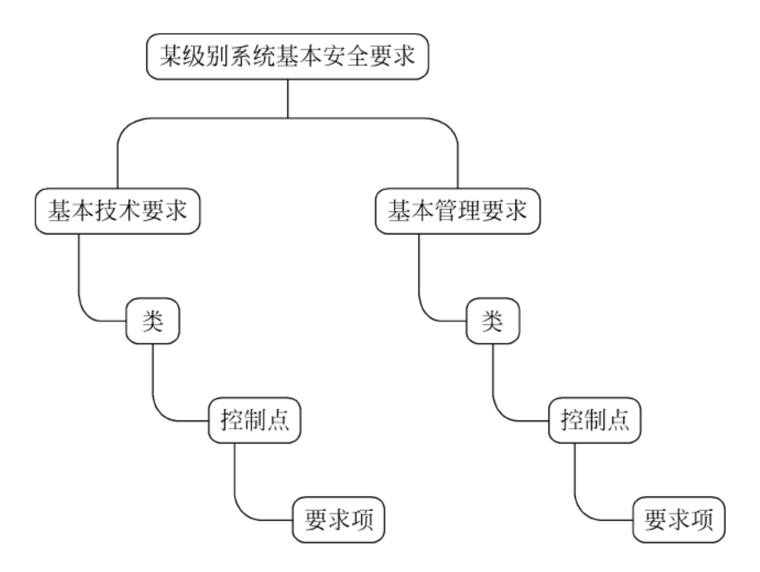


图 9-5 某级别系统等级保护能力的结构

根据《基本要求》中对第 1～5 级的基本安全要求，做了如表 9-5 所示的不同级别系统控制点和要求项的差异汇总，可以看出信息安全等级保护的基本安全要求具有如下特点。

（1）控制点逐级增加。逐级在同一类的控制点增加。

例如，第 3 级基本要求在第 2 级基本要求的基础上，技术方面，在控制点上增加了网络恶意代码防范、剩余信息保护、软件容错、抗抵赖等。管理方面，增加了系统备案、安全测评、监控管理和安全管理中心等控制点。第 4 级基本要求在第 3 级基本要求的基础上，技术方面，在系统和应用层面控制点上增加了安全标记、可信路径。

（2）要求项逐级增加。主要表现在不同级别的同一控制点的要求项逐级增多，项目增加，要求增强。

例如，对“身份鉴别”，第 1 级要求“进行身份标识和鉴别”，第 2 级增加要求“口令复杂度、登录失败保护等”，第 3 级则要求“采用两种或两种以上组合的鉴别技术”。

（3）要求项逐级增强。主要表现在要求项的范围逐级增大，要求也逐级细化，要求的粒度也逐级细化，增强了要求的强度。

表 9-5　信息安全等级保护基本安全要求差异汇总

安全要求类	类/层面	控制点				要求项			
		第 1 级	第 2 级	第 3 级	第 4 级	第 1 级	第 2 级	第 3 级	第 4 级
基本技术要求	物理安全	7	10	10	10	9	19	32	33
	网络安全	3	6	7	7	9	18	33	32
	主机安全	4	6	7	9	6	19	32	36
	应用安全	4	7	9	11	7	19	31	36
	数据安全及备份恢复	2	3	3	3	2	4	8	11
基本管理要求	安全管理制度	2	3	3	3	3	7	11	14
	安全管理机构	4	5	5	5	4	9	20	20
	人员安全管理	4	5	5	5	7	11	16	18
	系统建设管理	9	9	11	11	20	28	45	48
	系统运维管理	9	12	13	13	18	41	62	70
合计		48	66	73	77	85	175	290	318
级差			18	7	4		90	115	28

4. 信息安全等级保护的实施和设计

《定级指南》确定出系统等级以及业务信息安全性等级和业务服务保证性等级后，需要按照相应等级，根据《基本要求》选择相应等级的安全保护要求进行系统建设实施。

《信息系统安全等级保护实施指南(信安字[2007]10)》(以下简称《实施指南》)介绍和描述了实施信息系统等级保护过程中涉及的阶段、过程和需要完成的活动，通过对过程和活动的介绍，使大家了解信息系统实施等级保护的流程方法，以及不同角色在不同阶段的作用等。

1) 信息安全等级保护实施概述

《实施指南》规定了信息系统安全等级保护实施过程中应遵循自主保护原则、重点保护原则、同步建设原则以及动态调整原则。

在信息系统安全等级保护实施过程中各部门和相关机构等都要按照国家信息安全等级保护的相关管理规范和技术标准来履行相应的职责，信息系统安全等级保护实施过程中涉及的各类角色和职责如表 9-6 所示。

表 9-6　信息系统安全等级保护实施过程中涉及的角色和职责

角色和机构	相关部门	主要职责
国家管理部门	公安机关	负责信息安全等级保护工作的监督、检查、指导
	国家保密工作部门	负责等级保护工作中有关保密工作的监督、检查、指导
	国家密码管理部门	负责等级保护工作中有关密码工作的监督、检查、指导
	国务院信息化工作办公室及地方信息化领导小组办事机构	负责等级保护工作的部门间协调
	其他有关职能部门	涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理

续表

角色和机构	相关部门	主要职责
信息系统主管部门	—	负责督促、检查和指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作
信息系统运营和使用单位	—	(1) 负责确定其信息系统的安全保护等级，有主管部门的，应当报其主管部门审核批准； (2) 根据已经确定的安全保护等级，到公安机关办理备案手续，进行信息系统安全保护的规划设计； (3) 开展信息系统安全建设或者改建工作； (4) 制定、落实各项安全管理制度，定期对信息系统的安全状况、安全保护制度及措施的落实情况进行自查，选择符合国家相关规定的等级测评机构，定期进行等级测评； (5) 制定不同等级信息安全事件的响应、处置预案，对信息系统的信息安全事件分等级进行应急处置
信息安全服务机构	—	负责协助信息系统运营、使用单位完成等级保护的相关工作，包括确定其信息系统的安全保护等级、进行安全需求分析、安全总体规划、实施安全建设和安全改造等
信息安全等级测评机构	—	(1) 负责根据信息系统运营、使用单位的委托或根据国家管理部门的授权，协助信息系统运营、使用单位或国家管理部门，对已经完成等级保护建设的信息系统进行等级测评； (2) 对信息安全产品供应商提供的信息安全产品进行安全测评
信息安全产品供应商	—	(1) 负责开发符合等级保护相关要求的信息安全产品，接受安全测评； (2) 按照等级保护相关要求销售信息安全产品并提供相关服务

《实施指南》介绍了信息系统安全等级保护实施的基本流程，如图 9-6 所示。

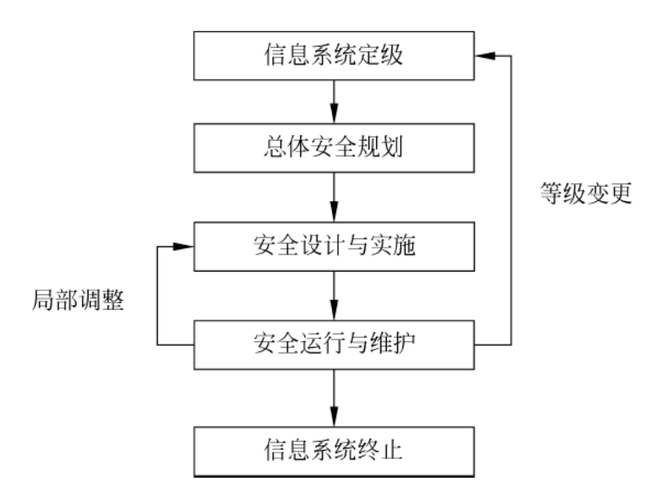


图 9-6 信息系统安全等级保护实施的基本流程

在安全运行与维护阶段，信息系统因需求变化等原因导致局部调整，而系统的安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施

安全措施，确保满足等级保护的要求；但信息系统发生重大变更导致系统安全保护等级变化时，应从安全运行与维护阶段进入信息系统定级阶段，重新开始一轮信息安全等级保护的实施过程。

在信息安全等级保护的实施过程中，如安全设计与实施等阶段的工作还要参考《信息系统等级保护安全设计技术要求(GB/T 24856—2009)》(以下简称《技术要求》)，该标准提出了信息系统等级保护安全设计的技术要求，包括第 1～5 级信息系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求，以及定级系统互联的设计技术要求，明确了体现定级系统安全保护能力的整体控制机制。《技术要求》用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构登记开展信息系统等级保护安全技术设计。

2）信息安全等级保护实施的特点

《实施指南》正文由 9 章和 1 个附录构成，从第 5 章开始就以信息系统安全等级保护建设实施的基本流程为主要线索，定义了信息系统等级保护实施的主要阶段和过程，再针对每个阶段介绍和描述主要的过程和实施活动，最后对每个活动说明实施主体、主要活动内容的输入输出等。

这里以信息系统定级阶段为例介绍《实施指南》对信息安全等级保护的实施工作是如何规定和指导的，让读者也能更清晰地了解《实施指南》的特点，如图 9-7 所示。

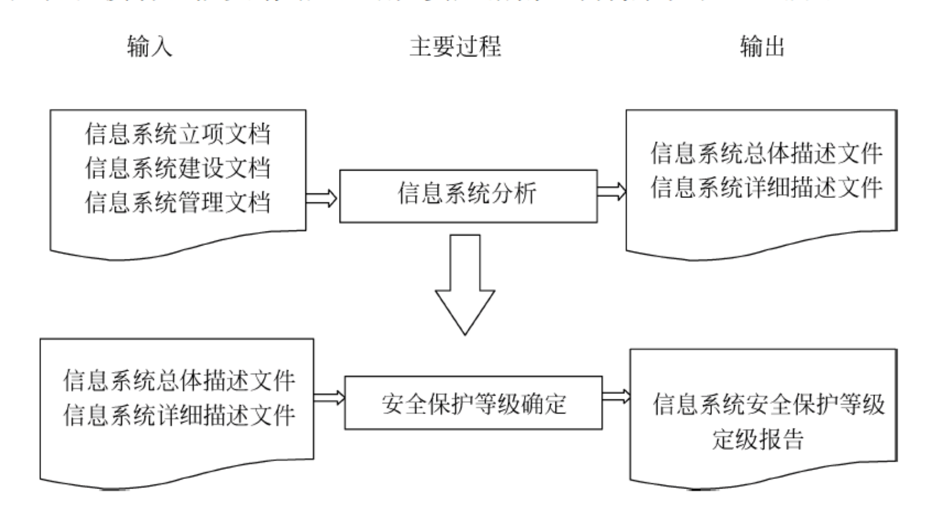


图 9-7　信息系统定级流程

【信息系统定级阶段分析】

以下内容摘自《实施指南》第 5 章。

5.1　信息系统分析

5.1.1　系统识别和描述

活动目标：

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统的立项、建设和管理文档。

活动描述：

本活动主要包括以下子活动内容：

a)识别信息系统的基本信息

略(具体参看《实施指南》)。

b)识别信息系统的管理框架

略(具体参看《实施指南》)。

c)识别信息系统的网络及设备部署

略(具体参看《实施指南》)。

d)识别信息系统的业务种类和特性

略(具体参看《实施指南》)。

e)识别业务系统处理的信息资产

略(具体参看《实施指南》)。

f)识别用户范围和用户类型

略(具体参看《实施指南》)。

g)信息系统描述

略(具体参看《实施指南》)。

活动输出：信息系统总体描述文件。

5.1.2 信息系统划分

……

可以看到《实施指南》就是按照阶段、过程、主要活动、子活动、活动的输入和输出这样的结构来进行每一个阶段的说明,让信息系统的使用单位对进行信息安全等级保护定级实施过程中需要进行的各事项更清晰。例如,从图 9-7 可以看出信息系统定级阶段包含 2 个过程,其中,过程 1 就是 5.1 信息系统分析,5.1.1 系统识别和描述就是过程 1 的主要活动,它包含了 a)～g)项子活动；过程 2 就是 5.1.2 信息系统划分,其余定级实施过程中涉及的各阶段包含的过程和主要活动以及子活动,请读者参阅《实施指南》的第 5～9 章的内容。

5. 信息安全等级保护的测评

信息系统建设完成后,运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评单位,依据《信息系统安全等级保护测评要求 GB/T 28448—2012》(以下简称《测评要求》)和《信息系统安全等级保护测评过程指南 GB/T 28449—2012》(以下简称《测评指南》)等技术标准,定期对信息系统安全等级状况开展等级测评。第 3 级信息系统应当每年至少进行一次等级测评,第 4 级信息系统应当每半年至少进行一次等级测评,第 5 级信息系统应当依据特殊安全需求进行等级测评。《测评要求》和《测评指南》构成了指导开展等级测评的标准规范。

《测评要求》从等级测评的原则、测评内容、测评强度、单元测评要求、整体测评要求、等级测评结论的产生方法等内容阐述,用于规范和指导测评人员如何开展等级测评工作。《过程指南》阐述了信息系统等级测评的测评过程,明确了等级测评的工作任务、分析方法以及工作结果等,包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动,用于规范测评机构的等级测评过程。

1) 信息系统等级保护测评的范围

《测评要求》规定了对信息系统安全等级保护状况进行安全测试评估的要求,包括对第 1 级信息系统、第 2 级信息系统、第 3 级信息系统和第 4 级信息系统进行安全测试评估的单

元测评要求和信息系统整体测评要求。本标准略去对第 5 级信息系统进行单元测评的具体内容要求，适用于信息安全测评服务机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的信息安全等级保护监督检查可以参考使用。

2）信息安全等级保护测评的原则

（1）客观性和公正性原则。测评工作虽然不能完全摆脱个人主张或判断，但测评人员应当在没有偏见和最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方法和过程，实施测评活动。

（2）经济性和可重用性原则。基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于这些结果还能适用于目前的系统，能反映目前系统的安全状态。

（3）可重复性和可再现性原则。无论谁执行测评，依照同样的要求，使用同样的方法，对每个测评实施过程的重复执行都应该得到同样的测评结果。可再现性体现在不同测评者执行相同测评的结果的一致性。可重复性体现在同一测评者重复执行相同测评的结果的一致性。

（4）符合性原则。测评所产生的结果应当是在对测评指标的正确理解下所取得的良好的判断。测评实施过程应当使用正确的方法以确保其满足了测评指标的要求。

3）信息安全等级保护测评的内容与方法

信息系统安全等级测评主要包括单元测评和整体测评两部分。单元测评是等级测评工作的基本活动，每个单元测评包括测评指标、测评实施和结果判定。其中，测评指标来源于《基本要求》中的第 5 级目录中的各要求项（参阅《测评要求》4.5 节内容），测评实施描述测评过程中使用的具体测评方法、涉及的测评对象和具体测评取证过程的要求，结果判定描述测评人员执行测评实施并产生各种测评数据后，如何依据这些测评数据来判定被测系统是否满足测评指标要求的原则和方法。整体测评是在单元测评的基础上，通过进一步分析信息系统的整体安全性，对信息系统实施的综合安全测评。整体测评主要包括安全控制点间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。整体测评需要与信息系统的实际情况相结合，因此全面地给出整体测评要求的全部内容、具体实施过程和明确的结果判定方法是非常困难的，测评人员应根据被测系统的实际情况，结合本标准的要求，实施整体测评。

测评方法指测评人员在测评实施过程中所使用的方法，主要包括访谈、检查和测试。其中，访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流，以帮助测评人员理解、分析或取得证据的过程；检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析，以帮助测评人员理解、分析或取得证据的过程；测试是测评人员使用预定的方法/工具，使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程。测评对象指测评实施的对象，即测评过程中涉及的信息系统的相关人员、制度文档、各类设备及其安全配置等。

4）信息安全等级测评的力度

测评力度是在测评过程中实施测评工作的力度，反映测评的广度和深度，体现为测评工作的实际投入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越

多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。投入越多，测评力度就越强，测评就越有保证。测评的广度和深度落实到访谈、检查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、检查和测试的投入程度的不同，如表 9-7所示。

表 9-7 信息安全等级测试力度

<table>
<tr><th colspan="2" rowspan="2">测评强度</th><th colspan="4">信息安全等级</th></tr>
<tr><th>第 1 级</th><th>第 2 级</th><th>第 3 级</th><th>第 4 级</th></tr>
<tr><td rowspan="2">访谈</td><td>广度</td><td>种类和数量上抽样，种类和数量都较少</td><td>种类和数量上抽样，种类和数量都较多</td><td>数量上抽样，基本覆盖</td><td>数量上抽样，基本覆盖</td></tr>
<tr><td>深度</td><td>简要</td><td>充分</td><td>较全面</td><td>全面</td></tr>
<tr><td rowspan="2">检查</td><td>广度</td><td>种类和数量上抽样，种类和数量都较少</td><td>种类和数量上抽样，种类和数量都较多</td><td>数量上抽样，基本覆盖</td><td>数量上抽样，基本覆盖</td></tr>
<tr><td>深度</td><td>简要</td><td>充分</td><td>较全面</td><td>全面</td></tr>
<tr><td rowspan="2">测试</td><td>广度</td><td>种类、数量和范围上抽样，种类和数量都较少，范围小</td><td>种类、数量和范围上抽样，种类和数量都较多，范围大</td><td>数量、范围上抽样，基本覆盖</td><td>数量、范围上抽样，基本覆盖</td></tr>
<tr><td>深度</td><td>功能测试/性能测试</td><td>功能测试/性能测试</td><td>功能测试/性能测试，渗透测试</td><td>功能测试/性能测试，渗透测试</td></tr>
</table>

信息安全等级保护要求不同安全保护等级的信息系统应具有不同的安全保护能力，满足相应等级的保护要求。为了检验不同安全保护等级的信息系统是否具有相应等级的安全保护能力、是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。第 1～4 级信息系统的测评力度反映在访谈、检查和测试等 3 种基本测评方法的测评广度和深度上，落实在不同单元测评中具体的测评实施上。

5）信息安全等级测评结果的重用

在信息系统中，有些安全控制可以不依赖于其所在的地点便可测评，即在其部署到运行环境之前便可以接受安全测评。一些商用安全产品的测评就属于这种安全测评。如果一个信息系统部署和安装在多个地点，且系统具有一组共同的软件、硬件、固件等组成部分，对这些安全控制的测评可以集中在一个集成测试环境中实施，如果没有这种环境，则可以在其中一个预定的运行地点实施，在其他运行地点的安全测评便可重用此测评结果。

在信息系统所有安全控制中，有一些安全控制与它所处于的运行环境紧密相关（如与人员或物理有关的某些安全控制），对其测评必须在分发到相应运行环境中才能进行。如果多个信息系统处在地域临近的封闭场地内，系统所属的机构在同一个领导层管理之下，对这些安全控制在多个信息系统中进行重复测评，可能是对有效资源的一种浪费。因此，可以在一个选定的信息系统中进行测评，其他相关信息系统可以直接重用这些测评结果。

6）信息安全等级保护测评的流程

信息安全等级保护测评实施的流程包括 4 个过程。

（1）测评准备。进行项目启动、信息收集和分析、工具和表单准备。

（2）方案的编制。测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、

测评实施手册开发、测评方案编制。

(3) 现场测评。现场测评准备(一般包括访谈、文档审查、配置检查、工具测试和实地察看),现场测评和结果记录、结果确认和资料归还。

(4) 分析与报告编制。单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成、测评报告编制。

9.2　信息安全法律法规及道德规范

9.2.1　信息安全涉及的相关法律问题

1. 计算机犯罪

1) 犯罪

《中华人民共和国刑法》第二章第十三条对犯罪的定义是：一切危害国家主权、领土完整和安全,分裂国家、颠覆人民民主专政的政权和推翻社会主义制度,破坏社会秩序和经济秩序,侵犯国有财产或者劳动群众集体所有的财产,侵犯公民私人所有的财产,侵犯公民的人身权利、民主权利和其他权利,以及其他危害社会的行为,依照法律应当受刑罚处罚的,都是犯罪。但是刑法第二章第十三条和第十六条又规定下面的两种情况不认为是犯罪：

(1) 情节显著轻微危害不大的,不认为是犯罪；

(2) 行为在客观上虽然造成了损害结果,但是不是出于故意或者过失,而是由于不能抗拒或者不能预见的原因所引起的,不是犯罪。

2) 计算机犯罪的相关法律条款

《中华人民共和国刑法》中关于计算机犯罪的规定有下面 3 个条款。

第二百八十五条　违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的,处三年以下有期徒刑或者拘役。

违反国家规定,侵入前款规定以外的计算机信息系统或者采用其他技术手段,获取该计算机信息系统中存储、处理或者传输的数据,或者对该计算机信息系统实施非法控制,情节严重的,处三年以下有期徒刑或者拘役,并处或者单处罚金；情节特别严重的,处三年以上七年以下有期徒刑,并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具,或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的,依照前款的规定处罚。

第二百八十六条　违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的,处五年以下有期徒刑或者拘役；后果特别严重的,处五年以上有期徒刑。

违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的,依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的,依照第一款的规定处罚。

第二百八十七条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者

其他犯罪的,依照本法有关规定定罪处罚。

以上三条分别对应非法侵入计算机信息系统罪、破坏计算机信息系统罪和利用计算机犯罪等三种计算机犯罪的表现形式。

从大的犯罪分类来看,计算机犯罪属于妨害社会管理秩序罪中的扰乱公共秩序罪。从犯罪的实质来看,刑法第二百八十五和二百八十六条所规定的犯罪是狭义的计算机犯罪或单纯的计算机犯罪,而刑法第二百八十七条则属于广义的计算机犯罪。

3）计算机犯罪的常见方法

(1) 以合法手段为掩护,查询信息系统中不允许访问的文件,或者侵入重要领域的计算机信息系统。

(2) 利用技术手段(包括利用网页与邮件、破坏账号和密码、设置木马程序、使用病毒程序、利用系统漏洞、程序缺陷和网络缺陷等)非法侵入重要的计算机信息系统,破坏或窃取计算机信息系统中的重要数据或程序文件,甚至删除数据文件或者破坏系统功能,直至使整个系统处于瘫痪。

(3) 在数据传输或者输入的过程中,对数据的内容进行修改,干扰计算机信息系统。

(4) 未经计算机软件著作权人授权,复制、发行他人的软件作品,或制作、传播计算机病毒,或制作传播有害信息等。

【计算机犯罪案例】

2013 年,辽宁省公安机关网安部门成功打掉一个非法入侵韩国网站盗窃韩国网民银行存款的特大团伙,共抓获犯罪嫌疑人 34 名,扣押涉案资金 200 余万元,车辆 16 台。

2013 年 1 月,辽宁省公安机关网安部门在工作中发现,网上有人发布"高价收购韩国银行资料"等信息。经查,自 2012 年起,黑龙江省网民王某龙(男,26 岁,黑龙江人)纠集他人在辽宁省丹东成立游戏工作室,通过互联网买卖韩国游戏币和韩国银行账户信息牟利,其贩卖的韩国游戏币主要来自王某(男,31 岁,贵州人)、孙某(男,27 岁,黑龙江人)犯罪团伙。进一步调查发现,王某,孙某犯罪团伙自 2012 年起从事盗窃韩国网民银行存款犯罪活动。其犯罪过程是：首先由王某联系黑客入侵韩国网站植入木马,当韩国网民浏览被入侵网站时,木马将自动植入网民使用的计算机,并窃取网民的网银账号和密码；然后,再由孙某登录受害人网银,将卡内存款直接转移至洗钱团伙提供的韩国银行卡并通过 ATM 取现,或者通过购买游戏点卡、充值卡等方式变相提现。据统计,仅半年时间,该犯罪团伙就先后对 100 余家韩国网站实施入侵,受到木马感染的计算机达千余台,盗窃韩国网民银行账号密码 4000 余组,盗窃资金折合人民币 1000 余万元。

2. 民事问题

在计算机及网络的使用等方面,不仅存在犯罪问题,也存在民事诉讼问题,任何人都可以对任何人、任何事提起民事诉讼。网络管理方面的漏洞、人为的误操作,人们在使用计算机和网络时有意或无意地侵权,都可能造成信息安全相关的民事问题。下面就通过一个简单的案例来说明信息安全方面的民事问题。

【民事问题案例】

本案系因持卡人泄露手机动态密码导致的电信诈骗,与其他同类电信诈骗引发的信用

卡纠纷案件一样,本案的核心焦点是持卡人与发卡行的过错划分问题。

具体案情如下。

李某系务农农民,2014 年办理了一张中国银行的信用卡,额度为 33 000 元。2015 年 12 月 9 日收到 04006695566 的银行客服电话,电话告知:尊敬的李先生,您在我行办理了一张信用额度的 33 000 元的信用卡,结合您的用卡情况可以为您提升信用卡额度。请提供您的卡号和身份证号以核对您的身份。李某说出后"客服"继续告知:核对成功,系统现在为您提升额度,您会收到验证码,请提供验证码我们为您操作。李某告知其收到的验证码后,"客服"提出由于系统较慢,提升的额度较大,程序较为复杂,建议删除已经收到的验证码,耐心等待。

就这样,李某按要求告知了多个验证码,并在"客服"指示下删除了短信,其实这些短信包括验证码短信及交易信息。就这样从 12 月 9 日至 12 月 14 日,李某连续接到这个电话,为其提升信用卡额度,李某均向"客服"告知了验证码。直至 12 月 14 日,李某回拨银行客服电话,才知自己接到的电话并非银行客服,而是电信诈骗分子利用任意显示号码打来的假客服电话。自己信用卡的资金已经被犯罪分子分 33 笔通过第三方支付平台支付。李某随即向银行提出质疑,冻结该卡,并向当地公安机关报案。

李某认为诈骗分子精准知道自己姓名及在中国银行办理了 33 000 元的信用卡,并且其接到的 0406695566 电话与被告客服电话 406695566 极其相似,骗子要求其提供身份证号及卡号核对身份的要求也是各家银行日常管理中经常会使用的,所以李某无法识别骗子的身份。最重要的是,中国银行在李某办卡及用卡时均未向其进行手机验证码可以交易的风险提示,银行在未经李某同意的情况下开通第三方支付,才导致李某被骗,银行存在严重过错,应该赔偿其资金损失。李某遂将银行起诉到法院,要求银行赔偿其全部资金损失。

最后法院判决如下:

(1) 认为原告所持信用卡发生支出交易产生的资金损失应按照双方责任进行分担。

(2) 原告在接到非被告客服电话后,未谨慎甄别即按照对方要求提供校验码,是产生他人利用第三方平台发生交易的主要原因,原告负有主要过错,应当对损失承担 70% 的主要责任。

(3) 被告在办理信用卡时未告知原告持卡风险,在发送非汇款、付款等交易校验码时未尽到风险提示义务,故被告在开办信用卡及服务中也存在瑕疵,负有次要过错,应对损失承担 30% 的次要责任。

3. 隐私问题

隐私问题是信息安全和保密中所涉及的一个非常重要的问题,隐私问题在个人、组织中都存在。信息安全隐私越来越受到人们的关注,利用法律手段有效保护组织和个人的隐私具有非常重要的意义。下面通过一个简单的案例来说明信息安全方面的隐私问题。

【隐私问题案例 1】

英国一位 21 岁的黑客,由于前女友移情别恋,愤而将与前女友的照片和录像"大白于天下",张贴在被其黑掉的站点上,结果因此被法院判了五个月的牢狱。这是属于个人隐私的案例。

【隐私问题案例2】

这不是个人隐私问题,涉及统计局CPI数据(国家宏观经济数据)泄露事件,是属于组织隐私数据的问题。

具体案情如下:

在北京市检察机关2011年"举报宣传周"活动新闻发布会上,市检察院反渎职侵权局局长张华伟披露,北京检方已介入CPI数据泄露一案。目前,包括国家统计局办公室一名秘书在内的5名相关人员均已被立案侦查。

新闻发布会上,记者提问CPI数据被泄露一案的最新进展,市检察院反渎职侵权局局长张华伟就此介绍称,对于媒体披露的CPI数据泄露问题,目前泄露国家秘密的问题比较突出。对于这起案件,检察机关已会同国家保密部门进行调查,目前已经立案5件,涉及5人。

张华伟随后解释称,由于涉案的5人分别来自不同部门,因此立了5个案子。这其中就包括国家统计局新闻发言人盛来运此前披露的"国家统计局办公室一秘书涉嫌泄露国家秘密案"。

有媒体称,今年3—4月份,国家统计局办公室一名秘书与央行研究局宏观经济研究处一副研究员因涉嫌数据泄密被有关部门带走调查。而今年6月8日,路透社再次抢先发布我国经济数据,预测中国5月份CPI较上年同期上涨5.4%,将追平3月份创下的32个月高位;彭博社也发布经济学家对宏观数据的预测值称,5月份的中国CPI同比涨幅为5.5%,这与国家统计局官方发布的中国5月CPI相关数据一致。

据统计,2008年以来,路透社已累计7次精准地"蒙对"了我国的月度CPI数据。提前泄露的数据信息,可能意味着可观的经济利益。多位业界分析人士在接受媒体采访时都认为,对一些经济机构来说,提前掌握宏观经济数据,有利于提前采取行动规避风险或谋取利益,尤其是一些和CPI联系紧密的金融产品,受CPI数据影响极大,提前获知CPI数据尤为重要。另外,从宏观层面上来说,CPI数据屡屡提前泄露,还会影响国家的经济安全。

9.2.2 我国的信息安全法律规范

1. 我国信息安全法律规范体系

1) 法律

法律就是由社会成员建立的以平衡个体自主权利的一套规则。法律大部分来自一种文化道德规范,它定义了一些被社会认同的(且符合社会成员广泛接受的法则)的行为。

2) 法律规范

法律规范是由国家制定或者认可,并由国家强制力保证实施的规范,因而具有国家意志和国家权力的属性;法律规范是以规范法律权力和法律义务为内容,是具有完整逻辑结构的特殊行为规范;法律规范具有普遍约束力,并对任何在效率范围内的主题的行为指导和评价,使用同一标准。

所以,法律规范是由国家强制力来保证实施的,对我国所有公民具有约束力,任何人都需要遵守。

3）信息安全法律规范体系

信息安全法律规范指用于规范信息系统或与信息系统相关行为的法律法规。信息安全法律法规具有命令性、禁止性和强制性。命令性和禁止性要求法律关系主体应当从事一定行为的规范，其规定的行为规则的内容是确定的，不允许主体一方或双方任意改变或违反，具体强制性。如果不执行，就要受到一定的法律制裁。

我国在信息安全法律规范方面采取多级立法，主要通过三大体系给予信息安全保障，图 9-8 是我国信息安全法律规范体系的一个框架图。

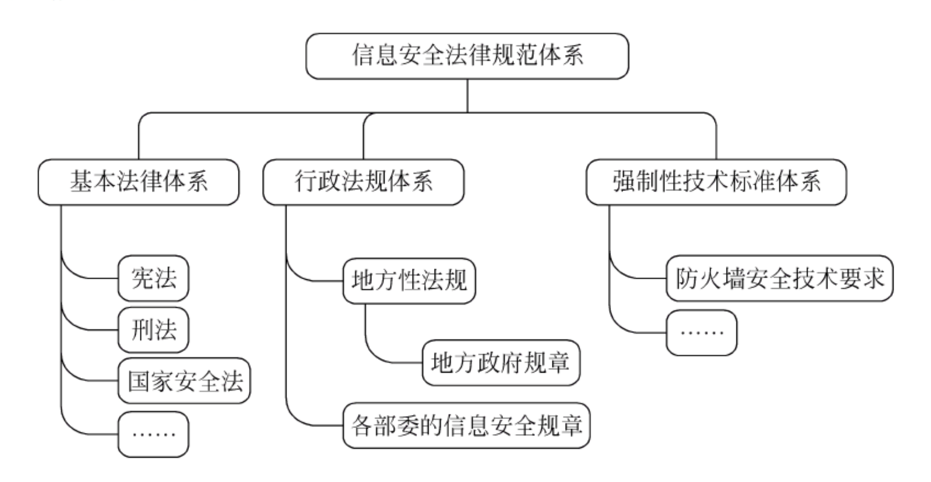


图 9-8 我国信息安全法律规范体系框架

（1）基本法律体系。

国家在许多基本法律中都设计了用于保护信息安全的条款，如《宪法》第四十条、《刑法》（部分条款）、《国家安全法》（部分条款）、《保守国家秘密法》等都做出了相关的规定。

（2）行政法规体系。

政府制定了一系列法规、规章，具体强化了对信息安全保护的力度。如《计算机信息系统安全保护条例》《互联网信息服务管理办法》等行政法规，公安部（安全专用产品等）、原信产部（互联网域名等）等各部委规章，《北京市信息化促进条例》《辽宁省计算机信息系统安全管理条例》等地方性法规，《北京市公共服务网络与信息系统安全管理规定》《上海市公共信息系统安全测评管理办法》等地方政府规章。

（3）强制性技术标准体系。

国家颁布了一系列技术标准，并且是强制性执行，从技术上规范了对信息安全的保护。这些标准的制定和内容在 9.1 节已经做了较详细的介绍。

2. 信息安全法律规范的法律地位

保障信息安全无论对一个国家还是对一个组织而言都是一个复杂的系统工程，需要多管齐下，综合治理。目前普遍认为，信息安全技术、法律法规和信息安全标准是保障信息安全的三大支柱。

国家、地方以及相关部门针对信息安全的需求，制定与信息安全相关的法律法规，从法律的层面来规范人们的行为，使信息安全工作有法可依，使相关违法犯罪行为能得到处罚，促使组织和个人依法制作、发布、传播和使用信息，从而达到保障信息安全的目的。

(1) 信息安全立法的必要性和紧迫性。

① 没有信息安全,就没有完全意义上的国家。

② 国家对信息资源的支配和控制能力,将决定国家的主权和命运。

③ 对信息的强有力控制是在世界格局中信息战能获胜的保证。

④ 信息安全保障能力已经是21世纪综合国力、经济竞争力和生成发展能力的重要组成部分。

(2) 信息安全法律规范的作用。

① 指引作用。法律作为一种行为规范,为人们的某种行为提供了一种模式,指引人们可以这样行为、必须这样行为或不得这样行为。

② 评价作用。用法律判断、衡量人们的行为是否是合法或违法以及违法性质和程序的作用。

③ 预测作用。当事人可以根据法律预先估计到其将如何行为以及某行为在法律上的后果。

④ 教育作用。能通过法律的实施对人们将来的行为产生一些影响。

⑤ 强制作用。法律对违法行为具有制裁、惩罚的作用。

9.2.3 我国的信息安全法律法规

目前,我国已建成起了基本的信息安全法律法规体系,根据党中央、国务院有关文件精神,起草并制定信息安全的相关法律是建立我国信息安全监督管理长效机制的重要保障,但随着信息安全形势的发展,信息安全立法的任务还非常艰巨,许多相关法规还在进一步完善。本书就介绍部分我国重要的信息安全的法律法规。

1.《宪法》第二章公民的基本权利和义务第四十条

宪法是依法治国的根本大法,是我国一切法律的基础依据。因此,信息化建设和信息安全都要从根本上遵循宪法。

宪法中同信息安全相关是第二章公民的基本权利和义务第四十条,规定公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要,由公安机关或者检察机关依照法律规定的程序对通信进行检查外,任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。

2. 中华人民共和国电子签名法

《中华人民共和国电子签名法》是为了规范电子签名行为,确立电子签名的法律效力,维护有关各方的合法权益而制定的法律。

《中华人民共和国电子签名法》由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于2004年8月28日通过,自2005年4月1日起施行。当前版本为2015年4月24日第十二届全国人民代表大会常务委员会第十四次会议修订。具体内容可参考《中华人民共和国电子签名法(2015年修订)》的原文。

3. 中华人民共和国计算机信息系统安全保护条例

《中华人民共和国计算机信息系统安全保护条例》是为了保护计算机信息系统的安全,

促进计算机的应用和发展，保障社会主义现代化建设的顺利进行而制定的法规，1994 年2 月 18 日，《中华人民共和国计算机信息系统安全保护条例》由中华人民共和国国务院令第 147 号发布，根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》修订，自 2011 年 1 月 8 日起实施，共五章三十一条，具体内容可参考《中华人民共和国计算机信息系统安全保护条例》的原文。

【破坏计算机信息系统案例】

被告人李××为牟取非法利益，以修改大型互联网网站域名解析指向的方法，劫持互联网流量访问相关赌博网站，获取境外赌博网站广告推广流量提成，导致某知名网站不能正常运行，访问量锐减。

上海市徐汇区人民检察院提起公诉后，人民法院认定李××的行为构成破坏计算机信息系统罪，结合量刑情节，判处李××有期徒刑五年。该案的起诉和判决，明确了修改域名解析服务器指向、强制用户偏离目标网站或网页进入指定网站或网页，造成计算机信息系统不能正常运行的域名劫持行为，属于破坏计算机信息系统。

4. 计算机信息网络国际联网安全保护管理办法

《计算机信息网络国际联网安全保护管理办法》是由中华人民共和国国务院于 1997 年 12 月 11 日批准，公安部于 1997 年 12 月 16 日公安部令（第 33 号）发布，于 1997 年 12 月 30 日起实施，根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》修订，共五章二十五条，具体内容可参考《计算机信息网络国际联网安全保护管理办法》的原文。

9.2.4　信息安全从业人员的道德规范

从信息安全问题的发展历史可以发现，很多重大信息安全事件的始作俑者与普通的暴力刑事罪犯是有一定差别的。他们往往有着较好的教育背景，但却因为缺乏道德的约束而利用自己的知识和技术来实施犯罪。所以教育体系和整个社会在培养知识人才的同时应该加强伦理道德的教育，提倡良好的信息使用规范和网络交流礼仪，引导人们将信息技术知识都运用到对社会有益的工作中去。

增强职业道德规范是计算机信息安全中人员安全的一个重要内容，是法律行为规范的补充，是非强制性的自律要求，其目的是用来规范各类信息的使用。所以，作为信息安全从业人员必须要保障因特网的运行安全；维护国家安全和社会稳定；维护社会主义市场经济秩序和社会管理秩序；保护个人、法人和其他组织的人身、财产等合法权利。

1. CISP 职业道德准则

注册信息安全专业人员（CISP）都必须严格履行其职责并遵守以下道德规范。

1）维护国家、社会和公众的信息安全

（1）自觉维护国家信息安全，拒绝并抵制泄露国家秘密和破坏国家信息基础设施的行为。

（2）自觉维护网络社会安全，拒绝并抵制通过计算机网络系统谋取非法利益和破坏社会和谐的行为。

(3) 自觉维护公众信息安全,拒绝并抵制通过计算机网络系统侵犯公众合法权益和泄露个人隐私的行为。

2) 诚实守信,遵纪守法

(1) 不通过计算机网络系统进行造谣、欺诈、诽谤、弄虚作假等违反诚信原则的行为。

(2) 不利用个人的信息安全技术能力实施或组织各种违法犯罪行为。

(3) 不在公众网络传播反动、暴力、黄色、低俗信息及非法软件。

3) 努力工作,尽职尽责

(1) 热爱信息安全工作岗位,充分认识信息安全专业工作的责任和使命。

(2) 为发现和消除本单位或雇主的信息系统安全风险做出应有的努力和贡献。

(3) 帮助和指导信息安全同行提升信息安全保障知识和能力,为有需要的人谨慎、负责地提出应对信息安全问题的建议和帮助。

4) 发展自身,维护荣誉

(1) 通过持续学习保持并提升自身的信息安全知识。

(2) 利用日常工作、学术交流等各种方式保持和提升信息安全实践能力。

(3) 以 CISP 身份为荣,积极参与各种证后活动,避免任何损害 CISP 声誉形象的行为。

2. 通行道德规范

1) 美国计算机伦理协会规定的计算机用户在网络系统中应遵守的 10 条行为准则

(1) 不应使用计算机危害他人。

(2) 不应干涉他人的计算机工作。

(3) 不应窥探他人的计算机文件。

(4) 不应使用计算机进行盗窃活动。

(5) 不应使用计算机做伪证。

(6) 不应复制或使用没有付费的版权所有软件。

(7) 不应在未经授权或在没有适当补偿的情况下使用他人的计算机资源。

(8) 不应挪用他人的智力成果。

(9) 应该注意你编写的程序或设计的系统所造成的社会后果。

(10) 使用计算机时应该总是考虑到他人并尊重他人。

2) 中国互联网协会的文明上网自律公约

自觉遵纪守法,倡导社会公德,促进绿色网络建设;

提倡先进文化,摒弃消极颓废,促进网络文明健康;

提倡自主创新,摒弃盗版剽窃,促进网络应用繁荣;

提倡互相尊重,摒弃造谣诽谤,促进网络和谐共处;

提倡诚实守信,摒弃弄虚作假,促进网络安全可信;

提倡社会关爱,摒弃低俗沉迷,促进少年健康成长;

提倡公平竞争,摒弃尔虞我诈,促进网络百花齐放;

提倡人人受益,消除数字鸿沟,促进信息资源共享。

9.3 小　　结

随着信息技术的不断发展和社会信息化进程的不断深入，信息技术本身的脆弱性和复杂性也日益呈现出来。信息安全事件和问题不断暴露，受到了政府和社会的广泛关注。各国纷纷研制和颁布信息安全相关标准与法律法规，我国也会对信息安全的标准和法律法规建设相当重视，已经建成一套基本满足我国经济和社会发展需要的标准和法律体系，为促进国民经济和社会发展发挥了积极作用。掌握相关标准和法律法规，使得信息安全从业人员能够有据可依、有法可循；了解相关标准和法律法规，对于规范信息系统使用者的行为是有必要的。

习　　题

1. 什么是计算机系统？请指出这个定义是在哪个标准或者法律规范中定义的。

2. 简述 GB 17859—1999 标准中第 1 级与第 2 级在安全保护能力上的差别。

3. 请参阅《信息系统安全等级保护基本要求(GB/T 22239—2008)》，统计出不同等级各类基本要求的控制点的情况。

4. 请参阅《信息系统安全等级保护实施指南(信安字[2007]10)》，归纳信息安全等级保护实施时各阶段的主要活动及输入和输出。

5. 以某一个组织或单位为例，描述该组织信息系统安全等级保护工作需要。

6. 我国的信息安全法律规范的体系主要包括哪几个方面？

7. 列举 1～2 个你所知道的信息安全方面的法律案例，并指出案例中涉及的法律法规。

8. 简述信息安全法律规范的作用。

9. 如果你是一个信息安全从业人员，请简述你应该从哪些方面做好工作。

第 10 章　信息安全工程案例

本章学习目标：

- 了解信息安全工程的系统概要及结构。
- 了解基于信息安全工程方法学的实践案例。

10.1　系 统 概 要

网上购物已成为人们生活中不可缺少的一种生活方式。网上书城系统是一种具有交互功能的商业信息系统，它在网络上建立一个虚拟的购物商场，使购物过程变得轻松、快捷、方便，同时为有效控制商场运营的成本开辟了一个新的销售渠道。

本系统 BookApp 是一个基于 B/S 架构的网上书城系统，为用户提供网上购书服务，并使其用户可以在线支付。它包括网站前台的购物系统和后台的数据库管理系统。具体来说，整个系统包含了图书发布、图书搜索、用户管理、订单处理、在线意见提交、后台管理等功能模块，实现了一个网上书城系统应该具备的基本功能。

整个 BookApp 系统的流程如图 10-1 所示，整个系统流程涵盖了用户注册、用户登录、查找图书、结账、生成订单以及查询订单、支付等。

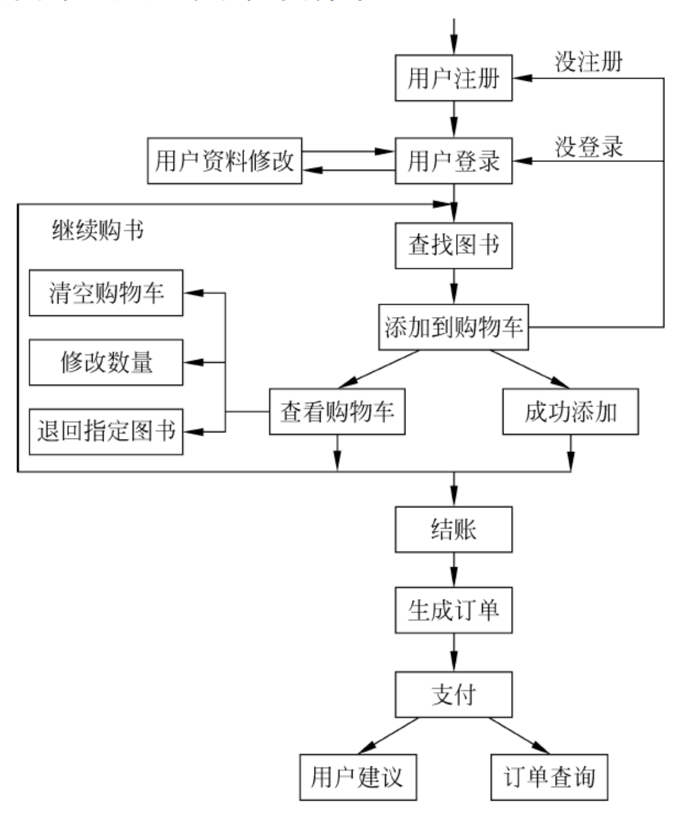


图 10-1　网上书城 BookApp 应用系统流程

10.2　系统结构

10.2.1　系统体系结构

所构建的网上书城系统整体平台是一个典型的 B/S 平台架构，由 Web 服务器平台、数据库服务器平台及客户端组成，如图 10-2 所示。

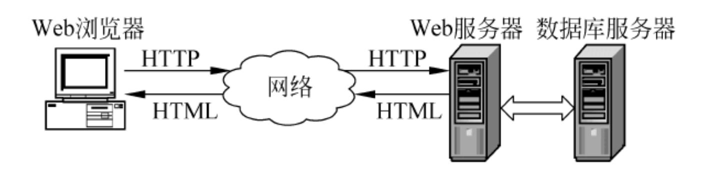


图 10-2　BookApp B/S 架构展示

10.2.2　系统功能结构

BookApp 系统主要可分为前台及后台两个部分。前台包括了用户管理、图书显示、收银台、订单查询、购物车、网上调查等 6 大模块。用户通过系统前台提供的功能模块可以注册并登录用户账户、查看图书、购买图书、支付，如图 10-3 所示。

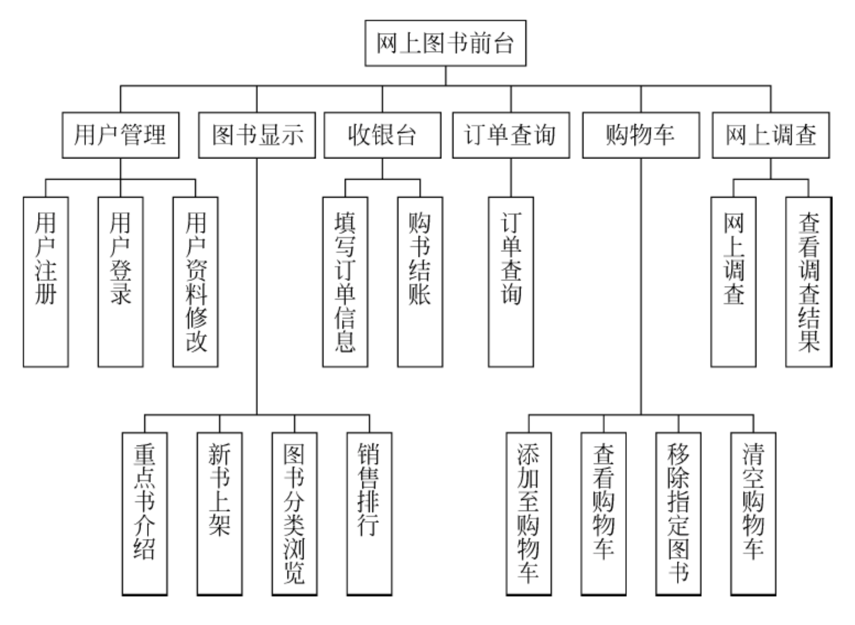


图 10-3　BookApp 系统前台模块图

系统的后台则包括了退出，图书管理、用户管理、公告管理、订单管理、网上调查、意见反馈等 6 大模块。管理员通过使用自己的管理员账户登录系统后台，利用提供的操作模块，更加具体地管理用户信息、图书信息、公告信息、订单信息。BookApp 系统后台模块如图 10-4 所示。

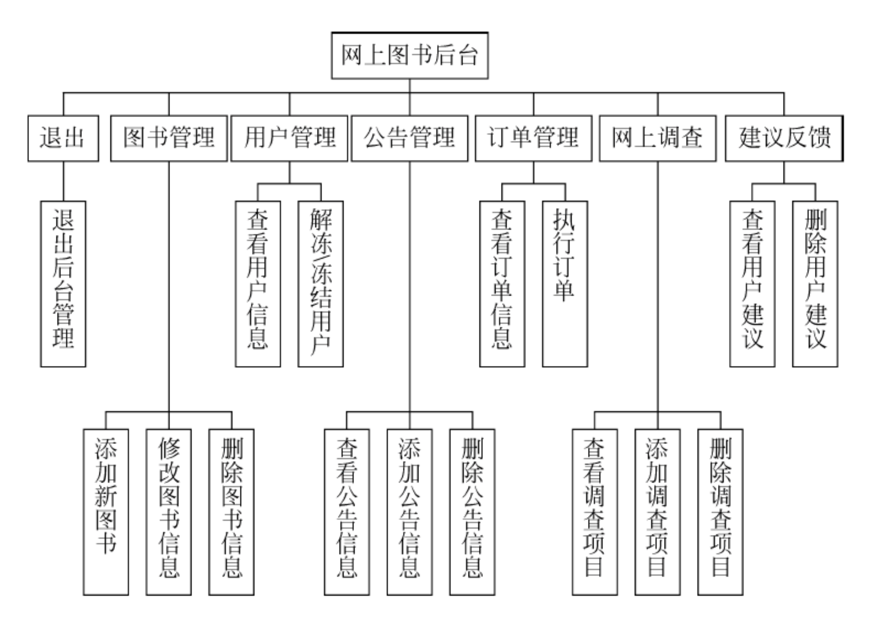


图 10-4 BookApp 系统后台模块图

10.3 系统安全风险分析

10.3.1 系统主要资产和关键业务信息

1. 系统主要资产

BookApp 网上书城系统主要的资产清单如下。

(1) Internet 基础设施。

(2) 电子商务基础平台。

(3) 硬件(PC 服务器和小型机)。

(4) 操作系统。

(5) Web 服务器、数据库服务器、邮件服务器。

(6) 图书信息。

(7) 客户信息。

2. 关键业务信息

BookApp 网上书城系统是在网络上建立一个 24 小时不打烊的网上书城,避免了挑选图书的烦琐过程,使购书过程变得轻松、快捷、方便,很适合现代人快节奏的生活;同时又能有效地控制书店运营的成本,开辟了一个新的销售渠道。

在网上书城整个使用过程中有很多信息在商家和买家之间传输,如买家的订单信息、商家的订单确定信息以及客户的银行账务信息等,这些都是 BookApp 的关键业务信息。

在后台数据库中应该存储着大量的图书信息供买家查询、选择等,这些图书信息也是必不可少的业务信息。

当用户注册该系统时,要填写一些个人信息,对于 BookApp 整个交易,这些客户信息也是关键的业务信息。

10.3.2　可能攻击源综合性分析

网络时代大潮的来临,使越来越多的人通过 Internet 进行商务活动。网上书店是随着网络技术的发展而出现的一种新型图书销售渠道,它通过人与电子通信方式的结合,依靠计算机网络,以通信技术为基础,实现图书销售的网上交易。这种销售方式得到了越来越多人的推崇,而正因为这样,导致了安全问题也变得越来越突出。特别是这几年,网络安全事件不断攀升,电子商务金融成了攻击目标,以网页篡改和垃圾邮件为主的网络安全事件正在大幅攀升,而网上书城也面临着同样的安全问题。

电子商务面临的安全威胁主要体现在如下方面。

1. 信息在网络的传输过程中被截获

攻击者可能通过互联网、公共电话网、在电磁波辐射范围内安装接收装置等方式,截获传输的机密信息,或通过对信息流量和流向、通信频度和长度等参数的分析,获取有用信息,如消费者的银行账号、密码等。

2. 传输的文件可能被篡改

攻击者可能从 3 个方面破坏信息的完整性。

(1) 篡改,即改变信息流的次序,更改信息的内容,如购买商品的出货地址。

(2) 删除,即删除某个消息或消息的某些部分。

(3) 插入,即在消息中插入一些信息,让接收方读不懂或接受错误的信息。

3. 伪造电子邮件

(1) 虚开网站和商店,给用户发电子邮件,收订货单。

(2) 给伪造的用户发恶意的电子邮件,耗尽商家资源,使合法用户不能正常访问网络资源,使有严格时间要求的服务不能及时得到响应。

(3) 伪造用户发大量的电子邮件,窃取商家的商品信息和用户信用等信息。

4. 假冒他人身份

(1) 冒充他人身份,如冒充领导发布命令、调阅密件。

(2) 冒充他人消费、栽赃。

(3) 冒充主机欺骗合法主机及合法用户。

(4) 冒充网络控制程序,套取或修改使用权限、密钥等信息。

(5) 接管合法用户,欺骗系统,占用合法用户的资源。

5. 不承认已经做过的交易(即交易的抵赖)

(1) 发消息者事后否认曾经发送过某条信息或内容。

(2) 收消息者事后否认曾经收到过某条消息或内容。

(3) 购买者做了订货单不承认。

(4) 商家卖出的商品因价格差而不承认原有的交易。

6. 网络蠕虫

网络蠕虫是一种可以不断复制自己并在网络中传播的程序。这种程序利用互联网上计算机系统的漏洞进入系统,自我复制,并继续向互联网上的其他系统进行传播。蠕虫的不断

蜕变并在网络上的传播,可能导致网络被阻塞的现象发生,从而致使网络瘫痪,使得各种基于网络的电子商务等应用系统失效。

7. 拒绝服务攻击

拒绝服务攻击是指在互联网上控制多台或大量的计算机针对某一个特定的计算机进行大规模的访问,使得被访问的计算机穷于应付来势凶猛的访问而无法提供正常的服务,使得电子商务这类应用无法正常工作。拒绝服务攻击是黑客常用的一种行之有效的方法。如果所调动的攻击计算机足够多,则更难进行处置。尤其是被蠕虫侵袭过的计算机,很容易被利用而成为攻击源,并且这类攻击通常是跨网进行的,加大了打击犯罪的难度。

8. 密码攻击

通过多种不同方法实现,包括蛮力攻击(brute force attack)、特洛伊木马程序、IP 欺骗和报文嗅探。尽管报文嗅探和 IP 欺骗可以捕获用户账号和密码,但密码攻击通常指反复地试探、验证用户账号或密码。这种反复试探称之为蛮力攻击。通常蛮力攻击使用运行于网络上的程序来执行,并企图注册到共享资源中,例如服务器。当攻击者成功地获得了资源的访问权,就拥有了和那些被破解账户用户相同的权限。如果这些账户有足够多的特权,那么攻击者就可以为将来的访问创建一个后门,从而不用担心被破解账户的任何身份和密码的改变。

10.3.3 系统对威胁存在的脆弱性分析

针对上述所提出的可能攻击源分析,可以把 BookApp 系统面临的威胁分为 6 种,分别是欺骗(spoofing)、篡改(tampering)、否决(repudiation)、信息泄露(information disclosure)、拒绝服务(denial of service)及权限提高(elevation of privilege)。现在分别针对这 6 种类型的威胁,对系统在面临威胁时候所存在的脆弱性做出研究和分析。

1. 威胁 1:欺骗

如果没有完善的身份验证机制,那么欺骗很容易成功。

2. 威胁 2:篡改

由于系统的后台数据库的数据是以明文形式存储的,而在信息传输过程中又没有任何的保密措施和完整性校验,因此只要攻击者使用网络嗅探器对网络进行嗅探,就能很容易地截获所传输的信息数据。而且当攻击者获得数据库的管理员权限并且成功入侵数据库之后,攻击者就可以随意地修改数据库中的任何信息。因此系统面对该威胁的脆弱性巨大,很容易被攻击者所利用。

3. 威胁 3:否决

由于系统没有相关的日志记录文件来记录系统的所有操作,并且没有要求发送者对其所发送的数据做数字签名,因此很容易遭到否决。所以,系统面对该威胁的脆弱性巨大,很容易被攻击者所利用。

4. 威胁 4:信息泄露

该威胁主要来源于管理层面,由于内部管理措施不当,造成了相关信息的泄露。而在技术上,主要是由于未对系统和信息进行加密,从而给攻击者提供了监听、窃取的机会,所以该

威胁很容易被人利用，系统脆弱性很大。

5. 威胁 5：拒绝服务

攻击者需要寻找大量的“肉机”，同时还要隐藏自身的 IP 的地址，其所付出的代价很大；由于系统的防火墙设置规则过于简单，没有针对拒绝服务的规则设置，因此，当面对拒绝服务的威胁时，系统几乎无抵抗能力。

6. 威胁 6：权限提高

利用缓冲区溢出等手段本身需要较高的技术支持，而且所需要的代价比较高昂，攻击成功的可能性不大。所以系统对该类威胁存在的脆弱性比较小，但是也不容忽视，因为一旦攻击成功，对系统所造成的伤害将是非常巨大的。

10.3.4　系统面临的安全风险综述

针对上述威胁和系统对威胁存在的脆弱性，还可以采用定性、定量或定性加定量的方式进一步分析系统面临的安全风险，最后得出系统面临的安全风险如下。

(1) 遭遇欺骗攻击。

(2) 信息被非法篡改。

(3) 遭遇对方否决。

(4) 私密信息被泄露。

(5) 遭到拒绝服务。

(6) 权限被非法提高。

10.4　BookApp 系统安全需求

10.4.1　计算机安全

计算机是一种硬件设备，硬件设备难免出现故障，一旦出现，将会影响电子商务系统的运行。特别是计算机的硬盘，一旦损坏，数据就会丢失，损失就无法挽回，需要对计算机硬件和数据进行备份。计算机系统安全主要考虑提高用于电子商务系统的计算机硬件可靠性和稳定性。

10.4.2　网络层安全需求

网络是用户进行数据交换、信息传递的主要途径。通过网络，用户可以访问网络中不同的计算机系统。网络安全主要是考虑限制用户对用于 BookApp 系统的计算机的访问权限，防止未授权的用户对系统的访问以及越权访问。

网络层安全主要解决企业网络互联时和在网络通信层安全问题，需要解决的问题如下。

(1) BookApp 系统网络进出口控制(即 IP 过滤)。

(2) BookApp 系统网络和链路层数据加密。

(3) 安全检测和报警、防杀病毒。

1. 网络进出口控制

需要对进入 BookApp 网站进行管理和控制,通过防火墙或虚拟网段进行分割和访问权限的控制。同样需要对内网到公网进行管理和控制,要达到授权用户可以进出内部网络,防止非授权用户进出内部网络这个基本目标。

2. 网络层与链路层数据加密

对关键应用需要进行链路层数据加密。

3. 安全检测和报警、防杀病毒

安全检测是实时对公开网络和公开服务器进行安全扫描和检测,及时发现不安全因素,对网络攻击进行报警。这主要是提供一种监测手段,保证网络和服务的正常运行。

(1) 及时发现来自网络内外对网络的攻击行为。

(2) 详细地记录攻击发生的情况。

(3) 当发现网络遭到攻击时,系统必须能够向管理员发出报警消息。

(4) 当发现网络遭到攻击时,系统必须能够及时阻断攻击的继续进行。

(5) 对防火墙进行安全检测和分析。

(6) 对 Web 服务器检测进行安全检测和分析。

(7) 对操作系统检测进行安全检测和分析。

需要采用网络防病毒机制来防止网络病毒的攻击和蔓延。严格地讲,防杀病毒属于系统安全需求范畴。

10.4.3 应用层安全需求

应用层的安全需求是客户应以自己的身份进行授权的操作,并保证自己的账户资源不被别人窃取,具体描述如下。

(1) 会员客户和企业电子商务服务器的双向身份鉴别——防止双向欺骗和假冒。

(2) 会员账户资源的授权访问控制——只能做授权范围内的操作。

(3) 资源的保密性和完整性——防止会员客户的口令、账户信息被网上窃听。

(4) 防止否认和抵赖——为业务仲裁提供法律依据。

(5) 账户资源访问的监视和审计。

10.4.4 后台管理的安全需求

所谓后台管理是指企业内部对 BookApp 系统的数据库、应用服务器等系统进行的日常管理工作,这些工作直接涉及客户保密信息。在管理过程中,系统管理员也要进行身份认证和授权管理,这样可以将内部风险降到最低限度。

10.4.5 BookApp 交易安全需求

BookApp 系统交易过程中,商家要发布产品信息,确认订购信息,收货款;客户要获取产品信息,传递订购信息,支付货款。买卖双方都存在安全问题,其中主要包括交易信息安全、支付安全和诚信安全。

1. 交易信息安全

交易信息包括商家的产品信息和订单确认信息、客户的订单信息。交易信息具有机密性,不能被篡改。交易信息安全主要是防止交易信息被截获或截获后被破译,以及防止数据被恶意篡改和破坏。

2. 支付安全

支付信息主要是客户的银行账号、交易金额,以及个人识别码(PIN)和电子货币信息。支付过程中必须保证这些信息的安全。同时,对商家来说,可能存在虚假订单,假冒者以客户名义订购货物,而要求客户付款;对客户来说,可能存在欺骗性网站,盗取客户敏感信息,导致资金被窃取。如何保证客户支付信息安全以及买卖双方身份的真实性,是支付安全主要考虑的问题。

3. 诚信安全

当交易信息和支付信息有了安全保障,也并不能让买卖双方放心从事网上交易。电子商务的在线支付形式有电子现金、电子支票、信用卡支付。但是采用这几种方式,都要求客户先付款,商家再发货。这样客户付款以后,会担心收不到货物或者收到劣质的货物。如果是先发货,然后付款,那么商家会担心客户是否会付款。

10.5　安全技术手段和方法

BookApp 系统的关键是保证交易数据和交易过程的安全,Internet 本身的开放性使 BookApp 系统面临各种各样的安全威胁。要解决安全问题,要求 BookApp 系统具备以下功能。

(1) 防止交易信息被非法截获或读取的保密性。

(2) 防止交易信息丢失并保证信息传递次序统一的完整性。

(3) 防止假冒身份在网上交易和诈骗的可靠性。

(4) 防止交易各方对已做交易无法抵赖的抗否认性以及原子性等安全要求。

根据 BookApp 系统信息安全性要求,对 BookApp 系统的安全问题进行了层次分析,提出了 BookApp 系统的安全框架体系结构。

BookApp 系统的安全框架体系结构是保证 BookApp 数据安全的一个完整的逻辑结构,由 5 部分组成,如图 10-5 所示。此安全体系由网络服务层、加密技术层、安全认证层、交易协议层、应用系统层组成。从图 10-5 中的层次结构可以看出,下层是上层的基础,为上层提供技术支持,上层是下层的扩展与递进,各层次之间相互依赖、相互关联构成统一整体,各层通过控制技术的递进实现 BookApp 的安全。

BookApp 系统是依赖网络实现的商务系统,需要利用 Internet 基础设施和标准,所以构成 BookApp 系统的安全框架的底层是网络服务层,它是 BookApp 系统应用的基础,并提供信息传送的载体和用户接入手段及安全通信服务,保证网络最基本的运行安全。为确保 BookApp 系统全面安全,必须建立完善的加密技术和认证机制。加密技术是保证 BookApp 系统安全所采用的最基本的安全措施,它用于满足 BookApp 对保密性的要求。安全认证层

中的认证技术是保证电子商务安全的必要手段,它对加密技术层中提供的多种加密算法进行综合运用,进一步满足 BookApp 系统对完整性、抗否认性、可靠性的要求。

在图 10-5 中所示的 BookApp 系统的安全框架体系中,加密技术层、安全认证层、交易协议层皆专为电子交易数据的安全而构筑。其中,交易协议层是加密技术层和安全认证层的安全控制技术的综合运用和完善,为 BookApp 系统的安全交易提供保障机制和交易标准。

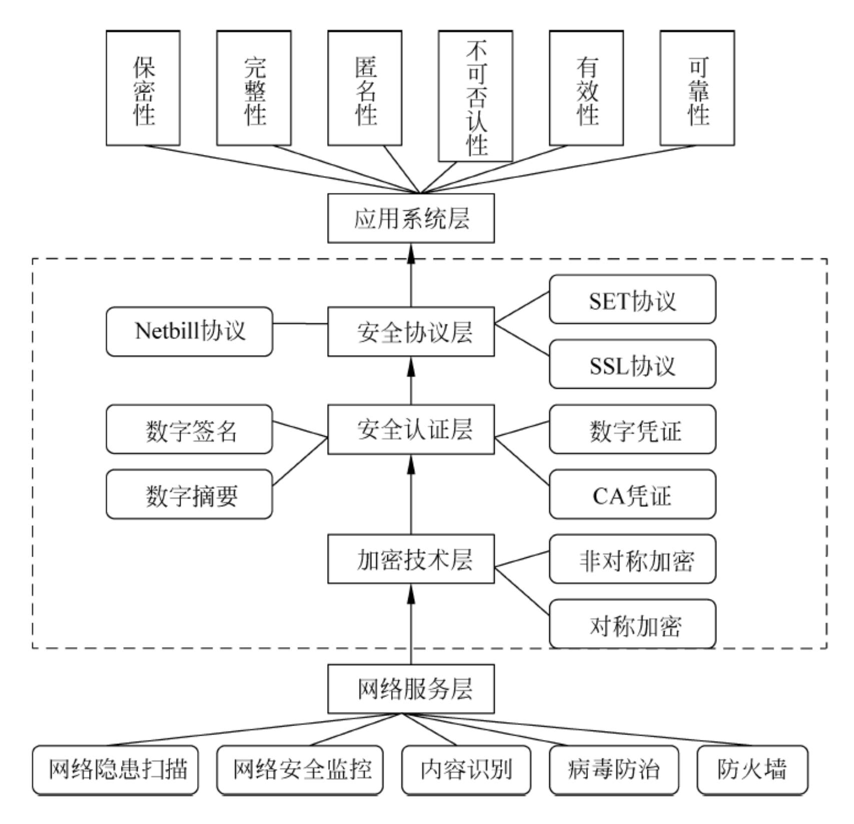


图 10-5　BookApp 系统安全体系结构

下面对各个层进行介绍。

10.5.1　网络服务层

网络基础结构层包括多厂商的网络服务及网络系统,用它们构成一种安全的、面向交易以及面向关系的通信网络联结。网络服务包括策略管理软件、地址管理软件、安全和网络管理软件。

1. 网络隐患扫描

作为一种积极主动的安全防护技术,网络隐患扫描在网络系统受到危害之前,可以及时发现安全隐患和漏洞,预先提供安全防护解决方案。

2. 网络安全监控

1）自动发现和控制非法的网络连接

功能描述:网络安全监控系统实时监控网内所有计算机的网络连接,一旦违反安全策略的网络连接出现,系统将向监控台实时报警,并根据预先设定的控制策略做出响应。

2）监控网内用户本地计算机的屏幕和操作

功能描述：根据网络监管员的指令，对网内用户本地计算机的屏幕和操作进行实时监控，包括用户计算机屏幕上的所用行为和用户键盘、鼠标的操作过程。

3）自动识别网内出现的陌生计算机

功能描述：网络安全监控系统能自动检测出不在当前监控范围内的计算机，并记录其信息和发出警报。

3. 内容识别

内容识别网络就是针对传输层到应用层进行网络的管理。如果一台交换机能够逐层解开通过的每一个数据包的每层封装，并识别出最深层的信息，那么它就具备了内容识别功能。要解决区分应用、动态分配资源和用户计费等问题，用网络识别设备分发业务流量是一个很好的途径。

4. 病毒防治

病毒的侵入必将对系统资源构成威胁，影响系统的正常运行。特别是通过网络传播的计算机病毒，能在很短的时间内使整个计算机网络处于瘫痪状态，从而造成巨大的损失。因此，防止病毒的侵入要比发现和消除病毒更重要。

5. 防火墙

防火墙是指一种将内部网和公众访问网分开的方法，是网络之间一种特殊的访问控制设施。在 Internet 网络与内部网之间设置的一道屏障，防止黑客进入内部网，由用户制定安全访问策略，抵御各种侵袭的一种隔离技术。在逻辑上，防火墙是一个分离器、一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。防火墙的安全技术主要包括包过滤技术、代理技术和地址迁移技术等。

10.5.2　加密技术层

加密技术是电子商务的最基本安全措施。所谓加密就是通过密码算法对数据进行转化，使之成为没有正确密钥任何人都无法读懂的报文。而这些以无法读懂的形式出现的数据一般被称为密文。为了读懂报文，密文必须重新转变为它的最初形式——明文，而含有用来以数学方式转换报文的双重密码就是密钥。在这种情况下即使一则信息被截获并阅读，这则信息也是毫无利用价值的。

1. 对称加密

对称加密（也称私钥加密）就是在数据加密和解密时使用相同的密钥。使用对称加密方法可以将加密处理简化，其优势也就在于简单快捷、密钥较短。与公钥算法相比，其算法也非常快，特别适用于对较大的数据流执行加密转换。但其不足之处在于通信双方必须事先告知密钥，否则接收方无法对数据进行解密，而密钥本身必须保证对未经授权的用户进行保密，因而在该传输过程中就会存在着密钥安全交换的问题。对称加密通常要与非对称加密一起使用。

2. 非对称加密

非对称加密（也称公钥加密）就是使用一个必须对未经授权的用户保密的私钥和一个可

以对任何人公开的公钥。非对称加密的优势在于密钥的可能值范围更大，解决了对称加密中私钥传递的不安全性，减少了对每个可能密钥尝试穷举的攻击性。同时，它可以创建数字签名以验证数据发送方的身份。但其不足之处在于非对称加密算法非常慢，不适合用来加密大量数据。

数据加密技术是信息安全的基本技术，在网络中使用的越来越广泛。密码技术的发展也将渗透到数字信息的每一个角落，与数据网络、通信系统的安全紧密联系在一起，提供更广泛、更有效的安全保护措施。

10.5.3　安全认证层

目前，仅有加密技术不足以保证电子商务中的交易安全，身份认证技术是保证电子商务安全不可缺少的又一重要技术手段，认证的实现包括数字证书、数字签名、数字摘要和数字时间戳等。

1. 数字证书

在一个电子商务系统中，所有参与活动的实体都必须用数字证书来表明自己的身份。数字证书一方面可以用来向系统中的其他实体证明自己的身份(每份数字证书都是经“相对权威的机构”签名的)，另一方面由于每份数字证书都携带着数字证书持有者的公钥，所以，数字证书也可以向接收者证实某人或某个机构对公开密钥的拥有，同时也起着公钥分发的作用。

2. 数字签名

所谓数字签名，就是只有信息的发送者才能产生的，别人无法伪造的一段数字串，它同时也是对发送者发送的信息的真实性的一个证明。签署一个文件或其他任何信息时，签名者首先须准确界定要签署内容的范围。然后，签名者软件中的哈希函数将计算出被签署信息唯一的哈希函数结果值。最后使用签名者的私人密码将哈希函数结果值转化为数字签名，得到的数字签名对于被签署的信息和用以创建数字签名的私人密码而言都是独一无二的。

3. 数字摘要

通过使用单向散列函数将需要加密的明文“摘要”成一个固定长度(128b)的密文。该密文同明文是一一对应的，不同的明文加密成不同的密文，相同的明文其摘要必然一样。因此，利用数字摘要就可以验证通过网络传输收到的明文是否是初始的、未被篡改过，从而保证数据的完整性和有效性。

4. 数字时间戳

在电子商务中，需对交易文件的日期和时间信息采取安全措施，而数字时间戳服务(DTS service)专用于提供电子文件发表时间的安全保护，该服务由专门的机构提供。所谓的时间戳是一个经过加密后形成的凭证文档，共包括3部分：需要加盖时间戳的文件的摘要、DTS收到文件的日期和时间、DTS的数字签名。

10.5.4　交易协议层

除了各种安全控制技术外，电子商务的运行还需要一套完善的交易安全协议。不同交易协议的复杂性、开销、安全性各不相同，不同的应用环境对协议目标的要求也不尽相同。

目前,比较成熟的协议有 SET、SSL、IKP 等基于信用卡的交易协议,NetBill、NetCheque 等基于支票的交易协议,DigiCash、NetCash 等基于现金的交易协议,匿名原子交易协议,防止软件侵权和非法复制的基于 KPC 的电子软件分销协议等。下面介绍 SSL 协议和 SET 协议。

1. SSL 协议

SSL(Secure Socket Layer,安全套接层)协议是在网络传输层之上提供的一种基于非对称密钥和对称密钥技术的用于浏览器和 Web 服务器之间的安全连接技术。SSL 协议支持了电子商务关于数据的安全性、完整性和身份认证的要求,但它没有保证不可抵赖性的要求。

2. SET 协议

SET(Secure Electronic Transaction,安全电子交易协议)采用公钥密码体制和 X.509 数字证书标准,主要应用于 B2C 模式中保障支付信息的安全性。SET 协议本身比较复杂,设计比较严格,安全性高,能保证信息传输的机密性、真实性、完整性和不可否认性。

由于 SET 协议提供了消费者、商家和银行之间的认证,确保了交易数据的安全性、完整性、可靠性和交易的不可否认性,特别是保证不将消费者银行卡号暴露给商家等优点,因此它成了目前公认的信用卡/借记卡的网上交易的国际安全标准。

10.5.5　应用系统层

在应用系统层中,通过以上各种技术和方法的应用后,在保密性上,通过前面各个层面的数据保护措施,保证了数据的保密性,即不会被窃取而导致数据被其他非法分子所知晓。在完整性上,保证了数据的完整性,即防止单方面对交易信息的生成和修改。在匿名性上,保证了数据的匿名性,即对交易的内容、交易双方账号、密码不被他人识别和盗取。在不可否认性上,保证了数据的不可否认性,即在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。在有效性上,保证了数据的有效性,即信息在传输到交易双方后信息是真实有效的。在可靠性上,保证了数据的可靠性,即保证网上交易合同的有效性,防止系统故障、计算机病毒、黑客攻击。

用于保证 BookApp 系统的安全控制技术很多,层次各不相同,但并非是把所有安全技术简单地组合就可以得到可靠的安全。

如果清楚了如图 10-5 所示的技术层次,通过合理结合与改进,就可以从技术上实现系统的、有效的 BookApp 安全。

10.6　系统安全管理机构及制度

10.6.1　BookApp 系统安全机构设置

安全机构的设置对系统的管理安全起到了一个调控的作用,BookApp 系统主要设置有以下安全机构。

(1) 运维管理部。负责定期对系统的设施进行维护管理;对服务器的开机、关机等工

目前,比较成熟的协议有 SET、SSL、IKP 等基于信用卡的交易协议,NetBill、NetCheque 等基于支票的交易协议,DigiCash、NetCash 等基于现金的交易协议,匿名原子交易协议,防止软件侵权和非法复制的基于 KPC 的电子软件分销协议等。下面介绍 SSL 协议和 SET 协议。

1. SSL 协议

SSL(Secure Socket Layer,安全套接层)协议是在网络传输层之上提供的一种基于非对称密钥和对称密钥技术的用于浏览器和 Web 服务器之间的安全连接技术。SSL 协议支持了电子商务关于数据的安全性、完整性和身份认证的要求,但它没有保证不可抵赖性的要求。

2. SET 协议

SET(Secure Electronic Transaction,安全电子交易协议)采用公钥密码体制和 X.509 数字证书标准,主要应用于 B2C 模式中保障支付信息的安全性。SET 协议本身比较复杂,设计比较严格,安全性高,能保证信息传输的机密性、真实性、完整性和不可否认性。

由于 SET 协议提供了消费者、商家和银行之间的认证,确保了交易数据的安全性、完整性、可靠性和交易的不可否认性,特别是保证不将消费者银行卡号暴露给商家等优点,因此它成了目前公认的信用卡/借记卡的网上交易的国际安全标准。

10.5.5　应用系统层

在应用系统层中,通过以上各种技术和方法的应用后,在保密性上,通过前面各个层面的数据保护措施,保证了数据的保密性,即不会被窃取而导致数据被其他非法分子所知晓。在完整性上,保证了数据的完整性,即防止单方面对交易信息的生成和修改。在匿名性上,保证了数据的匿名性,即对交易的内容、交易双方账号、密码不被他人识别和盗取。在不可否认性上,保证了数据的不可否认性,即在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。在有效性上,保证了数据的有效性,即信息在传输到交易双方后信息是真实有效的。在可靠性上,保证了数据的可靠性,即保证网上交易合同的有效性,防止系统故障、计算机病毒、黑客攻击。

用于保证 BookApp 系统的安全控制技术很多,层次各不相同,但并非是把所有安全技术简单地组合就可以得到可靠的安全。

如果清楚了如图 10-5 所示的技术层次,通过合理结合与改进,就可以从技术上实现系统的、有效的 BookApp 安全。

10.6　系统安全管理机构及制度

10.6.1　BookApp 系统安全机构设置

安全机构的设置对系统的管理安全起到了一个调控的作用,BookApp 系统主要设置有以下安全机构。

(1) 运维管理部。负责定期对系统的设施进行维护管理;对服务器的开机、关机等工

(3) 三级人员安全管理要求。在二级要求的基础上,增强了对关键岗位人员的录用、离岗和考核要求,对人员的培训教育更具有针对性,对外部人员访问的要求更具体。

(4) 四级人员安全管理要求。在三级要求的基础上,提出保密要求和关键区域禁止外部人员访问的要求。

1) 人员录用

对人员的安全管理,首先在人员录用时便应进行条件符合性筛选。录用时应考虑的方面包括人员技术水平、身份背景、专业资格等。通过对这几方面的审查,判断录用与否。对于从事重要区域或部门的安全管理人员的聘用要求则应更高,一般应从内部人员中选用那些实践证明精干、忠实、可靠、认真负责、保守秘密的人员。

该控制点在不同级别主要表现如下。

(1) 一级。要求负责部门或人员对录用人员身份、专业等进行基本的审查。

(2) 二级。在一级要求的基础上,增加了对录用人员技能的考核,并与关键岗位人员签署保密协议的形式约束其职责。

(3) 三级。在二级要求的基础上,增加了对从事关键岗位人员更加严格的录用要求,并与全部员工签署保密协议。

2) 人员离岗

由于人员在离开本岗位或本机构前,具有一定的访问权限,并知晓其中部分信息,因此对人员离岗的管理要求同样非常重要。在离岗时,主要从硬件归还(设备、设施)和权限撤销两方面考虑要求。

该控制点在不同级别主要表现如下。

(1) 一级。要求对离岗人员进行设备归还和权限终止。

(2) 二级。在一级要求的基础上,增加了规范离岗过程的要求。

(3) 三级。与二级要求的基础上,增加了关键岗位人员离岗的要求。

(4) 四级。在三级要求的基础上,增加了制度化规范的要求。

3) 人员考核

对人员的考核,主要是为了保持各个岗位人员能时刻满足该岗位的技术能力需求,同时也是机构对所有人员技能的阶段性全面了解。其中,重点关注对关键岗位人员的审查和考核。

该控制点在不同级别主要表现如下。

(1) 一级。无此要求。

(2) 二级。要求对人员定期进行技能考核。

(3) 三级。在二级要求的基础上,增加考核结果处理和对关键岗位的考核要求。

(4) 四级。在三级要求的基础上,增加保密制度和保密检查要求。

4) 安全意识教育和培训

保证信息系统的安全,要注重对安全管理人员的培养,提高其安全防范意识,最终做到安全有效地防范。而当前绝大多数漏洞存在的原因在于管理员对系统进行了错误的配置,或者没有及时升级系统软件。为确保员工在日常工作过程中能时刻意识到信息安全的威胁

和利害关系，并支持机构的信息安全方针，应根据安全教育和培训计划对所有员工进行培训，使其认识到自身的责任，提高自身技能。培训的内容包括单位的信息安全方针、信息安全方面的基础知识、安全技术、安全标准、岗位操作规程、最新的工作流程、相关的安全责任要求、法律责任和惩戒措施等。

该控制点在不同级别主要表现如下。

(1) 一级。对人员进行基本的安全意识和责任教育。

(2) 二级。除一级要求外，增强对安全教育培训的正规化管理。

(3) 三级。在二级要求的基础上，侧重于不同岗位的安全教育培训和制度化要求。

5) 外部人员访问管理

外部人员包括向机构提供服务的服务人员，如软硬件维护和支持人员、贸易伙伴或合资伙伴、清洁人员、送餐人员、保安和其他的外包支持人员等。若安全管理不到位，外部人员的访问将给信息系统带来风险。因此，在业务上有与外部人员接触的需要时，应当对其适当进行临时管理，对于 BookApp 系统的核心部分应不允许外部人员的访问，以确保其安全性。

该控制点在不同级别主要表现如下。

(1) 一级。对外部人员访问要得到授权和审批。

(2) 二级。除一级要求外，增加了对外部人员的访问的监督、备案等过程管理要求。

(3) 三级。在二级要求的基础上，增加了访问书面申请、访问制度等，更加严格外部人员访问管理。

(4) 四级。除三级要求外，要求外部人员禁止访问关键区域。

2. 机房管理制度

计算机和网络机房是 BookApp 系统硬件资源的集中地，网络机房管理主要以加强机房物理访问控制和维护机房良好的运行环境为主。

(1) 机房钥匙要严格保管，不得随意转借，一旦丢失要及时报告并积极寻找，并采取有效措施予以补救。

(2) 无关人员未经批准不得进入机房，更不得动用机房设备、物品和资料，确因工作需要，相关人员需要进入机房操作时必须经过批准方可在管理人员的指导或协同下进行。

(3) 机房应保持清洁、卫生，温度、湿度适宜，机房内严禁吸烟，严禁携带无关物品尤其是易燃、易爆物品及其他危险品进入机房。

(4) 消防物品要放在指定位置，任何人不得随意挪动；机房工作人员要掌握防火技能，定期检查消防设施是否正常。出现异常情况应立即采取切断电源、报警、使用灭火设备等正确方式予以处理。

(5) 硬件设备要注意维护和保养，做到设备物卡相符、设备使用状态记录完整。

(6) 建立机房登记制度，对本地局域网、广域网的运行情况建立档案。未发生故障或未有故障隐患时，网管人员不可对中继、光纤、网线及各种设备进行任何调试，对所发生的故障、处理过程和结果等要做好详细记录。

(7) 网管人员应做好网络安全工作，严格保密服务器的各种账号，监控网络上的数据流，从中检测出攻击的行为并给予响应和处理。

(8) 网管人员要对数据实施严格的安全与保密管理,防止系统数据的非法生成、变更、泄露、丢失及破坏。网管人员应在数据库的系统认证、系统授权、系统完整性、补丁和修正程序方面实时修改。

(9) 网管人员对各种网络设备的使用需按操作程序或使用说明书进行。

(10) 经常对硬件设备进行检查、测试和修理,确保其运行完好。

(11) 所有贵重设备均由专人保管,专人使用,不得外借或由非专业人员单独操作。

(12) 中心机房的所有设备未经许可一律不得挪用和外借,特殊情况经批准后办理借用手续,借用期间如有损坏由借用单位或使用人员负责赔偿。

(13) 硬件设备发生损坏、丢失等事故,应及时上报,填写报告单并按有关规定处理。

(14) 中心机房及其附属设备的管理(登记)与维修由网管人员负责。设备管理人员每半年要核准一次设备登记情况。

(15) 中心机房主机(系统服务器)、网络服务器及其外围设备由网管人员每周进行一次例行检查和维护,尤其是设备供电、运行状态等要时常检查和维护。

(16) 软件要定期进行系统维护与备份,备份至少保持一式两套,并存放在温度、湿度适宜的磁介质库存中。

(17) 应用软件、应用数据应根据运行频率进行定期或不定期的备份工作,备份软件和数据应存放于的磁介质库存中。

(18) 应用软件的源程序除了在磁介质上备份以外,网管人员应自己进行备份,以防应用程序发生意外而难以恢复。

(19) 为了便于对系统软件进行应用与管理,机房中须备有与系统软件有关的使用手册和各种操作指南等资料,以便维护人员查阅。其资料未经许可,任何人不得带出机房。

(20) 应用软件人员应将项目的调研资料、各阶段的设计说明书、图表、源程序、应用系统运行流程图等进行分类归档,以便查阅。

(21) 当应用软件修改时,具体的功能修改、逻辑修改、程序变动等,都应有相应的文档记录,以备查阅。

(22) 为确保软件系统的安全,磁介质除了应有专人管理外,还应配备防火器具,确立防磁、防静电、防灰尘等有效措施(建筑上保证),磁介质保管要明确责任,遵守出入库制度。

(23) 网管人员应有较强的病毒防范意识,定期进行病毒检测(特别是服务器),发现病毒应立即处理。

(24) 采用国家许可的正版防病毒软件并及时更新软件版本。

(25) 未经领导许可,网管人员不得在服务器上安装新软件,若确实需要安装,安装前应进行病毒例行检测。

(26) 经远程通信传送的程序或数据,必须经过检测确认无病毒后方可使用。

(27) 中心机房安全是关系到行业安全的一件大事,是保证各个业务系统正常工作的前提条件,因此必须坚持定期进行安全检查。

(28) 中心机房自检每年进行一次,且须认真做好检查记录。

(29) 对检查中发现的问题将进行限期整改。

3. 运行安全制度

不仅在设计或者维护上要有制度，在运行上也同样需要安全制度。主要的运行安全制度如下。

（1）除中心网络管理机构负责人及其授权的维护人员外，其他单位或个人不得以任何方式试图进入内部网主、辅节点，服务器等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对内部网安全运行的破坏行为。

（2）内部网中对外发布信息的 Web 服务器中的内容必须经单位领导审核，由网络负责人从技术上开通其对外的信息服务。

（3）内部网各类服务器中开设的账户和口令为个人用户所拥有，中心网络管理机构人员对用户口令保密，不得向任何单位和个人提供这些信息。

（4）网络使用者不得利用各种网络设备或软件技术从事用户账户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

（5）中心机关组织内部施工、建设不得危害计算机网络系统的安全。

（6）内部网主、辅节点设备及服务器等发生案件，以及遭到黑客攻击后，中心网络管理机构必须在 8 小时内向公安机关报告。

（7）严禁在内部网上使用来历不明、引发病毒传染的软件；对于来历不明的可能引起计算机病毒的软件应使用公安部门推荐的杀毒软件检查、杀毒。

（8）任何个人不得在内部网及其联网计算机上传送危害国家安全的信息（包括多媒体信息），录阅传送淫秽、色情资料。

（9）中心网及子网的系统软件、应用软件及信息数据要实施保密措施。

（10）中心网络管理机构必须落实各项管理制度和技术规范，监控、封堵、清除网上有害信息。为了有效地防范网上非法活动，内部网要统一出口管理、统一用户管理，进出内部网访问信息的所有用户必须使用中心网络负责人设立的代理服务器、E-mail 服务器。

（11）中心网络中设立的服务器必须保持日志记录功能，历史记录保持时间不得低于 6 个月。负责服务器管理的网络管理人员必须按照有关管理部门要求登记内容，并按时上报有关信息。

4. 核心信息和资产访问制度

在应用系统中建立核心信息和资产访问制度是为了保证应用系统受控合法地使用。用户只能根据自己的权限大小来访问应用系统，不得越权访问。

（1）要求根据一定的控制策略来限制用户对系统资源的访问，控制粒度较粗。

（2）控制粒度细化，增加覆盖范围要求，并强调了最小授权原则，使得用户的权限最小化。

（3）增加了对重要信息设置敏感标记，并控制对其的操作。

（4）提出以标记的方式进行应用系统访问的控制。

从物理访问控制来说，系统机房出入口应安排专人值守，控制、鉴别和记录进入的人员，且需进入系统机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。从系统访问控制来说，对人员进行身份限制，在登录系统的时候根据身份的不同用不同的账号、密

码登录,并对系统有不同的访问控制权限,如管理员经过身份认证后可以访问核心资产并对数据做出修改,而普通用户只能查看一些通用信息,对关键数据是不可见并且不能修改的。

5. 备份恢复制度

BookApp 系统处理的各种数据(用户数据、系统数据、业务数据等)在维持系统正常运行上起着至关重要的作用。一旦数据遭到破坏(泄露、修改、毁坏),都会在不同程度上造成影响,从而危害到系统的正常运行。由于 BookApp 系统的各个层面(网络、主机、应用等)都对各类数据进行传输、存储和处理等,因此,对数据的保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。各个“关口”把好了,数据本身再具有一些防御和修复手段,必然将对数据造成的损害降至最小。

另外,数据备份也是防止数据被破坏后无法恢复的重要手段,而硬件备份等更是保证系统可用的重要内容,在高级别的信息系统中采用异地适时备份会有效地预防灾难发生时可能造成的系统危害。

保证数据安全和备份恢复主要从数据完整性、数据保密性、备份和恢复等 3 个控制点考虑。

(1) 对用户数据在传输过程提出完整性要求,能够检测出数据完整性受到破坏,同时能够对重要信息进行备份。

(2) 对数据完整性的要求增强,范围扩大。要求鉴别信息和重要业务数据在传输过程中都要保证其完整性。数据保密性要求实现鉴别信息存储保密性,数据备份增强,要求一定的硬件冗余。

(3) 对数据完整性的要求增强,范围扩大。增加了系统管理数据的传输完整性,不仅能够检测出数据受到破坏,并能进行恢复。对数据保密性要求范围扩大到实现系统管理数据、鉴别信息和重要业务数据的传输与存储的保密性,数据的备份不仅要求本地完全数据备份,还要求异地备份和冗余网络拓扑。

(4) 为进一步保证数据的完整性和保密性,提出使用专有的安全协议的要求。同时,备份方式增加了建立异地适时灾难备份中心,在灾难发生后系统能够自动切换和恢复。

数据完整性主要保证各种重要数据在存储和传输过程中免受未授权的破坏,这种保护包括对完整性破坏的检测和恢复。

主要制度是:能够对用户数据在传输过程的完整性进行检测,要求鉴别信息和重要业务数据在传输过程中都要保证其完整性,不仅能够检测出数据受到破坏,并能进行恢复,要求采用安全、专用的通信协议。

数据保密性主要从数据的传输和存储两方面保证各类敏感数据不被未授权的访问,以免造成数据泄露。

主要制度是要求能够实现鉴别信息的存储保密性,实现系统管理数据、鉴别信息和重要业务数据的传输与存储的保密性,要求采用安全、专用的通信协议。

所谓“防患于未然”,即使对数据进行了种种保护,但仍无法绝对保证数据的安全。对数据进行备份,是防止数据遭到破坏后无法使用的最好方法。

通过对数据采取不同的备份方式、备份形式等,保证系统重要数据在发生破坏后能够恢

复。硬件的不可用同样也是造成系统无法正常运行的主要原因。因此,有必要将一些重要的设备(服务器、网络设备)设置冗余。当主设备不可用时,及时切换到备用设备上,从而保证了系统的正常运行。如果有能力的话,对重要的系统也可实施备用系统,主应用系统和备用系统之间能实现平稳、及时地切换,主要是能够对重要数据进行备份,能够提供一定的硬件冗余,提供异地备份和冗余网络拓扑,建立异地适时灾难备份中心,在灾难发生后系统能够自动切换和恢复。

10.7 小 结

本章主要针对一个网上书城系统的安全问题进行研究及分析,从而给出一套安全解决方案,但由于时间和能力的限制,该安全解决方案还有很多地方需要进一步完善,从而使该系统能在一个安全的环境中被广泛应用。

参 考 文 献

[1] 陈庆华.系统工程理论与实践[M].北京：国防工业出版社，2009.
[2] 王金山，谢家平.系统工程基础与应用[M].北京：地质出版社，1996.
[3] 冯允成，等.系统工程基础[M].北京：北京航空航天大学出版社，1995.
[4] 杜瑞成，闫秀霞.系统工程[M].北京：机械工业出版社，1999.
[5] 徐斌.质量管理[M].北京：企业管理出版社，2001.
[6] 潘渔洲.现代企业质量管理[M].北京：经济管理出版社，1997.
[7] 胡子谷.质量管理[M].上海：上海交通大学出版社，2004.
[8] 李江蛟.现代质量管理[M].北京：中国计量出版社，2002.
[9] 杨一平，等.现代软件工程技术与CMM的融合[M].北京：人民邮电出版社，2002.
[10] 龚波.软件过程管理[M].北京：中国水利水电出版社，2003.
[11] 李伟波，刘永祥，王庆春.软件工程[M].武汉：武汉大学出版社，2006.
[12] 史济民，等.软件工程原理、方法与应用[M].北京：高等教育出版社，2002.
[13] 丁斌.项目管理教程[M].合肥：安徽科学技术出版社，2005.
[14] 蒋景楠.项目管理[M].上海：华东理工大学出版社，2006.
[15] 霍亚楼.项目管理基础[M].北京：对外经济贸易大学出版社，2008.
[16] 王雪青.国际工程项目管理[M].北京：中国建筑工业出版社，2000.
[17] 柳纯录.信息系统项目管理师教程[M].2版.北京：清华大学出版社，2008.
[18] 张焕国，崔竞松，王丽娜.ISSE在信息系统中的应用[J].计算机工程，2003，29(19).
[19] 冯肇瑞.安全系统工程的回顾与展望[J].中国安全科学学报，1992，2(3)：8-12.
[20] 蔡皖东，等，系统安全工程能力成熟度模型(SSE-CMM)及其应用[M].西安：西安电子科技大学出版社，2004.
[21] 杜跃进，崔宝林，张建荣.系统安全工程能力成熟度模型(SSE-CMM)[J].中国计算机报，2001(5)：22-25.
[22] 吴晓平，付钰.信息安全风险评估教程[M].武汉：武汉大学出版社，2011.
[23] 朱少彰.信息安全导论[M].北京：国防工业出版社，2010.
[24] 沈昌祥.信息安全工程导论[M].北京：电子工业出版社，2003.
[25] 刘莹，顾卫东.信息安全风险评估研究综述[J].青岛大学学报，2003，23(2)：28-33.
[26] 李志伟.信息安全风险评估及风险管理对策研究[D].北京：北京交通大学，2010.
[27] 陈忠文，麦永浩.信息安全标准与法律法规[M].2版.武汉：武汉大学出版社，2009.
[28] 陈湉，张彦超，赵爽.国际信息安全标准现状研究及对我国标准体系建设的思[J].信息安全与通信保密，2016：41-47.
[29] 黄元飞，栗欣.网络与信息安全标准研究现状及热点问题探讨[C].电信科学，2008，24(1)：19-25.
[30] 中国电子技术标准化研究院.云计算标准化白皮书[M].北京：中国电子技术标准化研究院，2014.
[31] 朱建平，李明.信息安全等级保护标准体系研究[J].信息安全标准与技术追踪，2005(5)：21-24.
[32] 宗言伟，马钦德，张健.信息安全等级保护政策和标准体系综述[J].信息通信技术，2010，6：58-62.
[33] 公安部信息安全等级保护评估中心.信息安全等级保护政策培训教程[M].北京：电子工业出版社，2010.
[34] 陈之赞.关于信息安全管理的法律问题研究[D].上海：复旦大学，2012.